前　言

数论（The Theory of Numbers）是数学的一个古老分支，它是研究数的性质，特别是整数性质的一门学科。在公元前三世纪，古希腊数学家欧几里德（Euclid，公元前330—公元前275）著的《几何原本》的第八、九、十篇就是专门记载历史上有关数论的成就。例如，用辗转相除法求最大公约数的步骤，至今仍称之为欧几里德算法，他还证明了素数个数的无穷性等等。我国早在公元前后的《孙子算经》里就提出“物不知其数”的问题：“今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何？答曰二十三”。这是世界上最早提出解同余式组

$$x \equiv 2 \pmod 3,$$
$$x \equiv 3 \pmod 5,$$
$$x \equiv 2 \pmod 7$$

的问题。关于解上述同余式组的定理，初等数论书中称为孙子定理，有的外文书中称为中国剩余定理（The Chinese Remainder Theorem）。

数论应该说是古希腊人首创的，十七世纪法国数学家费马（Fermat，1601—1665）对数论作出了巨大的贡献，他的工作决定了这门学科的早期研究方向。德国数学家高斯（Gauss 1777—1856）曾经说过：“数学是科学的皇后，数论是数学的皇后”，这说明，大数学家早就认识到数学在科学中享有的独特地位及数论在数学中享有的独特地位。

世界上的一切事物都不是孤立存在的。数论亦不例外，它并不孤立，而是与数学的其他分支有着密切的关系。例如，欧几里德用初等方法证明了素数的数目是无穷的，十八世纪瑞士数学家欧拉（Euler，1707—1783）用解析方法证明同一命题。高斯二次反转定律既可用初等方法亦可用拓扑方法来证明，近代国外某些数学家还把古老的费马大定理，转为可用拓扑方法来解决的问题。从使用数学方法的不同，数论可分为解析数论、代数数论和数的几何三个主要分支。

数论又称理论算术．整除性（可约性）理论、同余式论（实际上是整除性理论比较复杂的情况）等等都是乘法数论的内容；而把一个数表示成和的形式，如，不定方程的整数解问题、哥德巴赫（Goldbach）猜想、四个平方和问题（拉格朗日～Lagrange～定理）和华林（Waring）问题等等，都是加法数论的内容，加法数论亦称堆垒数论。

十九世纪以前，数论还仅是一系列孤立结果的罗列，1801年高斯的《算术探讨》(Disquisition Arithmetical)一书出版则标志了现代数论的开始．高斯的数论著作有三个主要思想：同余理论、代数数的引进、型的理论．同余理论是总结历史上费马、欧拉、拉格朗日和勒让得（Legendre）等数学家的成就，并引用了“≡”的符号。

整除概念可推广于“除数”为0，即$0|0$，$0\nmid a$（$a\neq 0$），若模m亦允许$m=0$，则以0为模的同余类有无穷多个，即$a\equiv a \pmod 0$，$a\neq b$时，$a\not\equiv b \pmod 0$，所以有理整数相等的关系是同余关系的一个特例．柯西（Cauchy）用i代替整系数多项式

$$f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n+\cdots$$

中的x，得到

$$f(i)\equiv(a_0-a_2+a_4-\cdots)+(a_1-a_3+a_5-\cdots)x$$
$$(\mathrm{mod}(i+1)).$$

柯西的这种思想，用多项式的同余式来定义复数。如实系数多项式

$$f(x)\equiv a+bx\ (\mathrm{mod}(x^2+1))$$

关于模 x^2+1 与 $a+bx$ 同余的任何多项式都表示同一复数 $a+bi$

高斯首先把 i 添加于有理整数环R，得到比R多两个单位（可逆元）±i 的一个二次整数环R〔i〕（R只有±1两个单位，而R〔i〕有±1，±i四个单位），并把合数、素数、同余等概念推广于R〔i〕。例如，$5=(1+2i)(1-2i)$ 在R〔i〕里是合数而不是素数。高斯还证明了，在R〔i〕中可用欧几里德除法求二整数的最大公因数。更广泛地对这些问题的研究产生了代数整数论，它有丰富的内容与方法，当时高斯本人也没有想到，代数数概念的引入与证明费马大定理是分不开的，康米尔（Kummer）把 x^p+y^p（p是素数）分解成

$$(x+y)(x+\alpha y)\cdots(x+\alpha^{p-1}y)$$

这里α是虚的 p 次单位根，也就是，α 是

$$x^{p-1}+x^{p-2}+\cdots+x+1=0 \qquad (1)$$

的一个根，这就把高斯的复整数理论推广到由（1）那样的方程引进代数数。

由于在R〔$\sqrt{-5}$〕中

$$6=2\cdot3=(1+\sqrt{-5})(1-\sqrt{-5}),$$

而2，3，$1+\sqrt{-5}$，$1-\sqrt{-5}$都是 R〔$\sqrt{-5}$〕中的素数，因此在二次整数环 R〔$\sqrt{-5}$〕中唯一分解定理不成立。但是若令 $\alpha=\sqrt{2}$，$\beta_1=(1+\sqrt{-5})/\sqrt{2}$，$\beta_2=(1-\sqrt{-5})/\sqrt{2}$，

则 $2=\alpha^2$， $3=\beta_1\beta_2$， 且

$$6=\alpha^2\beta_1\beta_2$$

就是唯一分解了．为了解决这个问题，1844年开始康米尔写了一系列论文，创立了理想数的理论，解决了唯一分解定理的存在问题．康米尔还用他的理想数成功地证明了费马大定理对许多素数是成立的．

狄德金采用与康米尔完全不同的方法来重建代数数域中的唯一分解定理，他用代数数类来定义理想，给出了一般的唯一分解定理（理想数的基本定理）．他还创立了现代代数数的理论，奠定了代数数论的基础．代数数论的工作在十九世纪以希尔伯特（Hilbert）的论代数数的著名报告为顶峰．他用新颖、漂亮的方法来重新整理早期的理论，其后，他和其他许多人大大地扩展了代数数论．

型理论的产生，肇源于丢番图（Diophantos）的思想，从研究整数的型表示，引入型等价的概念以及二元二次型的分类等．高斯在《算术探讨》的第五节中系统化并扩展了型的理论，打下研究数的几何的基础．

解析方法导入数论使数论得到很大的发展，欧拉、雅可比（Jacobi）都做了一些工作，解析数论的诞生更应归功于狄利克雷（Dirichlet，1805—1859）．为了证明欧拉和勒让得猜测：每一个算术序列

$$a,\ a+b,\ a+2b,\ \cdots,\ a+nb,\ \cdots (a,\ b)=1$$

中包含无穷多个素数，他引用了分析的方法．又，对不超过 x 的素数个数 $\pi(x)$ 的估值，欧拉、勒让得和高斯等人猜测：

$$\lim_{x\to\infty}\frac{\pi(x)}{x/\ln x}=1$$

在这个问题的研究中，也自然地引入了分析方法．

此外，还有用黎曼（Riemann）ζ函数

$$\zeta(z)=\sum_{n=1}^{\infty}\frac{1}{n^z}\text{（z为复数）}$$

来证明素数定理等。这些工作奠定了解析数论的基础。

本书共分九章，前六章是数论必不可少的基础知识。我们以欧拉括号和连分数为工具来处理初等数论的若干问题，并较全面地、系统地介绍同余式及同余式组解的存在、数量和解法。第七章代数整数，以二次整数为模型阐明代数整数与有理整数的异同。并在附录中介绍了规尺作图不能问题的判别法。第八章通过数论函数与素数分布，了解解析数论处理问题的方法。第九章介绍二元二次型的简单知识，初步给出求二次曲线上整点的方法。总之，本书主要是使读者初步了解什么是数论，并为进一步学习数论打好基础。作者长期在福建师大担任数论基础课程，深感数论对于数学爱好者的魅力之强，为了爱好者自学方便，使具备高中数学知识及初等微积分的读者都能卒读全书，在讲义的基础上尽量修改，做到通俗易懂、深入浅出以减少自学的困难。书末附有习题解答。

限于作者水平，本书的缺点与错误在所难免。敬希广大读者批评指正。

王杰官

1986年秋于福州

目　　录

第一章　整数的整除性理论

整除是数论中的重要概念，本章主要介绍整数的整除的概念和性质，以带余除法和辗转相除法为工具，建立最大公因数和最小公倍数的理论，并证明算术基本定理。此外，还介绍两个很常用的数论函数[x]、{x}，连分数和欧拉括号等内容。

第一节　整除的概念与性质

两个整数的和、差、积仍然是整数，但是一个非零整数去除另一个整数，所得的商却不一定是整数，因此我们有必要引进整除的概念。

我们约定，下面没有特别声明时，小写拉丁字母a，b，c，…，p，q，r，…等等都表示整数；符号“$\forall$”代表“任给”；“$\exists \cdots \ni$”读作“存在……使得”；“$A \Longrightarrow B$”表示“若有A，则有B”；“$A \Longleftrightarrow B$”是指“B是A的充要条件”。

定义1·1　设a，$b \neq 0$，若$\exists q \ni a = bq$，则称b整除a(a divisible by b)，记作

$$b \mid a.$$

或称a被b所整除，记作

$$a \vdots b.$$

此时称b是a的因数（factor）或约数（divisor），a是b的倍数（multiple）。

反之，若不存在这样的q时，则称b不整除a，记作

$b \nmid a$。

这时b不是a的因数，a不是b的倍数。

这个定义可用下列符号简单表示：

$a, b \neq 0, \exists q \ni a = bq \Longleftrightarrow b|a$。

因为在定义1·1中，并不要求存在的q是唯一的，所以关于整除的概念，必要时可以排除$b \neq 0$的限制，当$b=0$且$a \neq 0$时，$b \nmid a$；当$b=0$且$a=0$时，$b|a$，这时q不是唯一的。

整除有下列诸性质：

1° $a|b, b|a \Longrightarrow a = \pm b$。

证明 $a|b, b|a \Longrightarrow \exists q_1, q_2 \ni b = aq_1$, $a = bq_2 \Longrightarrow a = q_1 q_2 a \Longrightarrow q_1 q_2 = 1 \Longrightarrow q_1 = \pm 1$。

∴ $a = \pm b$。

2° $a|b, b|c \Longrightarrow a|c$。

证明 $a|b, b|c \Longrightarrow \exists q_1, q_2 \ni b = aq_1, c = bq_2 \Longrightarrow c = aq_1 q_2 \Longrightarrow a|c$。

3° $a|b_1, a|b_2, \cdots, a|b_n, \forall k_1, k_2, \cdots, k_n$
$\Longrightarrow a|k_1 b_1 + k_2 b_2 + \cdots + k_n b_n$*

证明 对n用数学归纳法证明之。

A) 当$n=1$时，显然结论成立。

B) 设$n=h$时，结论成立。即

$a|b_1, \cdots, a|b_h, \forall k_1, \cdots, k_h \Longrightarrow a|k_1 b_1 + \cdots + k_h b_h$。

当$n=h+1$时，若$a|b_1, \cdots, a|b_h, a|b_{h+1}$，$\forall k_1, \cdots, k_h, k_{h+1}$，则由归纳法假设及定义1·1，有

* “|”是表示前后二整数的一种关系，它不与“运算关系”连合使用，放在一个式子里。所以此式就是$a|(k_1 b_1 + k_2 b_2 + \cdots + k_n b_n)$的简写。

$\exists q_1 q_2 \ni k_1 b_1 + k_2 b_2 + \cdots + k_h b_h = aq_1$， $k_{h+1} b_{h+1} = aq_2$
$\Longrightarrow k_1 b_1 + \cdots + k_h b_h + k_{h+1} b_{h+1} = a(q_1 + q_2)$。

$\therefore \quad a | k_1 b_1 + \cdots + k_h b_h + k_{h+1} b_{h+1}$

所以 n 为任意自然数时结论成立。

我们把 $k_1 b_1 + \cdots + k_n b_n$ 叫做 $b_1, \cdots, b_n$ 的一个组合，则性质 3°指的是：若 $a | b_i (i = 1, \cdots, n)$，则 a 整除 $b_1, \cdots, b_n$ 的任意组合。由性质 3°立即推得

4° $\sum_{i=1}^{n} b_i = 0$，若 $a | \sum_{i=1}^{n} b_i - b_1$，

则 $a | b_j$，$(j = 1, 2, \cdots, n)$。

在一般的情形下，a 被 b 除时，我们有

定理 1·1 （带余除法）若 $\forall a, b > 0$，则 $\exists q, r \ni$

$$a = bq + r, \quad 0 \leqslant r < b \tag{1}$$

成立，并且 q 和 r 都是唯一的。

证明 作整数序列

$$\cdots, -3b, -2b, -b, 0, b, 2b, 3b, \cdots,$$

则由亚里士多德公理（Aristoteles，整数集是亚里士多德式的有序集）知，a 必在上面序列的某两项之间，即 $\exists q \ni qb \leqslant a < (q+1)b$ 成立，令 $a - qb = r$，则等式（1）成立。

设 q_1，r_1 亦满足（1），即

$$a = bq_1 + r_1, \quad 0 \leqslant r_1 < b$$

因而

$$bq_1 + r_1 = bq + r \Longrightarrow b(q_1 - q) = r - r_1 \Longrightarrow$$
$$\Longrightarrow b|q_1 - q| = |r - r_1|，而 |r - r_1| < b \Longrightarrow q_1 - q = 0$$
$$\Longrightarrow r = r_1, \quad q = q_1。$$

定义1·2 （1）中的q，r 分别叫做 a 被 b 除所得的不完

全商(incomplete quotient)和余数(remainder)，特别当 $r=0$时，q 叫做 a 被 b 除所得的商(quotient)，这时 $b|a$。

例1·1 设$b=7$，$a=-115$，则 $q=-17$，$r=4$，即$-115=7\times(-17)+4$，$0<4<7$。

当 $b=7$，$a=84$时，$q=12$，$r=0$，即$84=7\times12+0$，此时$7|84$。

第二节 最大公因数与最小公倍数

定义1·3 n个整数a_1，a_2，…，a_n，若$d|a_i$($i=1$，2，…，n)，则称 d 为a_1，a_2，…，a_n的一个公因数或公约数(common factor or commondivisor)，公因数中最大的一个称为a_1，a_2，…，a_n的最大公因数(greatest common factor)，记作

$$(a_1, a_2, \cdots, a_n).$$

若$(a_1, a_2, \cdots, a_n)=1$，则称$a_1$，$a_2$，…，$a_n$互素(relatively prime or coprime)或互质。若$(a_i, a_j)=1$ $(i\neq j=1, 2, \cdots, n)$，则称$a_1$，$a_2$，…，$a_n$两两互素(质)。

显然，若a_1，a_2，…，a_n两两互素，则a_1，a_2，…，a_n互素。反之不一定成立，例如，$(12, 15, 8)=1$，但$(12, 15)=3$，$(12, 8)=4$。

若$a_1=a_2=\cdots=a_n=0$，则任一整数都是它们的公因数，但是它们没有一个最大的公因数。若a_1，a_2，…，a_n不全为零，则存在一个最大公因数。

为了在讨论过程中，避免区别正负整数的麻烦，我们先证明

5° 若a_1，a_2，…，a_n是n个不全为零的整数，则

(i) $a_1, a_2, \cdots, a_n$ 与 $|a_1|, |a_2|, \cdots, |a_n|$ 的公因数相同；

(ii) $(a_1, a_2, \cdots, a_n) = (|a_1|, |a_2|, \cdots, |a_n|)$.

证明 设 d 是 $a_1, a_2, \cdots, a_n$ 的任一公因数，由定义1·3知

$d \mid a_i \ (i = 1, 2, \cdots, n) \Longrightarrow d \mid |a_i| \ (i = 1, 2, \cdots, n)$ 即 d 亦是 $|a_1|, |a_2|, \cdots, |a_n|$ 的公因数；反之也是显然的。特别是，若 $d = (a_1, a_2, \cdots, a_n)$，$d' = (|a_1|, |a_2|, \cdots, |a_n|)$，则 $d \mid |a_1|, d \mid |a_2|, \cdots, d \mid |a_n| \Longrightarrow d \leqslant d'$；且 $d' \mid a_1, d' \mid a_2, \cdots, d' \mid a_n \Longrightarrow d' \leqslant d$.

$\therefore \ d = d'$.

因为 $(0, b) = |b| \ (b \neq 0)$，所以下面不妨只在正整数范围内讨论最大公因数的问题．无特别声明本节下面出现的小写拉丁字母都代表正整数．

容易证明整除的下列诸性质：

6° $(a_i, a_j) = 1 \ (i \neq j = 1, 2, \cdots, n)$

$\Longrightarrow (a_1, a_2, \cdots, a_n) = 1$.

7° $b \mid a \Longrightarrow (a, b) = b, \ (b \neq 0)$.

8° 若 $a = bq + c$，则 a，b 的任一公因数都是 b，c 的公因数；反之，b，c 的任一公因数也都是 a，b 的公因数．特别是

$$(a, b) = (b, c).$$

下面介绍欧几里德算法（Euclidean algorithm）或称辗转相除法，并用以求两个正整数的最大公因数，$\forall a, b$，

由带余除法，得

$$\begin{cases} a = bq_1 + r_2, & 0 < r_2 < b; \\ b = r_2q_2 + r_3, & 0 < r_3 < r_2; \\ \cdots \quad \cdots \quad \cdots \quad \cdots; \\ r_{n-2} = r_{n-1}q_{n-1} + r_n, & 0 < r_n < r_{n-1}; \\ r_{n-1} = r_nq_n + r_{n+1}, & r_{n+1} = 0. \end{cases} \tag{2}$$

因为每进行一次除法，余数至少减少1，b是有限整数，故有限次进行带余除法后，必出现余数为0的情况。由性质8°及7°立得

$$(a, b) = (b, r_2) = (r_2, r_3) = \cdots = (r_{n-1}, r_n) = r_n.$$

定理1·2 任意正整数a和b，则$(a, b) = r_n$，r_n就是（2）中最后一个不等于0的余数。

系1 a，b的一切公因数，都是(a，b)的因数。

例1·2 求（－1859，1573）.

解

$q_2 = 5$	1573	1859	$1 = q_1$
	1430	1573	$2 = q_3$
	$r_3 = 143$	$r_2 =$ 286	
		286	
		0	

∴ （－1859，1573）＝（1859，1573）＝143.

系2 设a，b≠0都是整数。

(i) 若$m > 0$，则$(am, bm) = (a, b)m$;

(ii) 若$c > 0$，$c|a$，$c|b$，则$\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{(a, b)}{c}$.

(iii) $\left(\frac{a}{(a, b)}, \frac{b}{(a, b)}\right) = 1$.

证略.

系 3 n个正整数$a_1, a_2, \cdots, a_n$，若$(a_1, a_2)=d_2$，$(d_2, a_3)=d_3$，…，$(d_{n-1}, a_n)=d_n$，则

$$(a_1, a_2, \cdots, a_n)=d_n.$$

证明 ∵ $d_n|a_n$，$d_n|d_{n-1}$ 且 $d_{n-1}|a_{n-1}$

$\Longrightarrow d_n|a_{n-1}$，又 $d_{n-1}|d_{n-2}\Longrightarrow d_n|d_{n-2}$，

且 $d_{n-2}|a_{n-2}\Longrightarrow d_n|a_{n-2}$ 又 $d_{n-2}|d_{n-3}\Longrightarrow\cdots\Longrightarrow d_n|a_1$

∴ $d_n|(a_1, a_2, \cdots, a_n)$

$a_1, a_2, \cdots, a_n$的任一公因数d，显然$d|a_1$，$d|a_2\Longrightarrow d|d_2$，又$d|a_3\Longrightarrow d|d_3$，$\cdots\Longrightarrow d|d_n$.

∴ $d\leqslant|d|\leqslant d_n$.

因而d_n是$a_1, a_2, \cdots, a_n$的最大公因数，即

$$(a_1, a_2, \cdots, a_n)=d_n.$$

最大公因数，还有下列诸性质：

9° 若$(a, b)=1$，c为任意整数，则$(ac, b)=(c, b)$.

证明 $(ac, b)|ac$，$(ac, b)|bc\overset{\text{系}1}{\Longrightarrow}(ac, b)|(ac, bc)$.

由系2(i)知，$(ac, bc)=(a, b)|c|=|c|\Longrightarrow(ac, b)|c$且$(ac, b)|b\Longrightarrow(ac, b)|(c, b)$.

反之，显然$(c, b)|(ac, b)$

∴ $(ac, b)=(c, b)$.

10° $(a, b)=1$，$b|ac\Longrightarrow b|c$.

证明 因为$b|ac$，$(a, b)=1$，所以

$(ac, b)=|b|\Longrightarrow(ac, b)=(c, b)=|b|\Longrightarrow b|c$.

由10°立即推得

11° $(a_i, a_j)=1\ (i\neq j=1, 2, \cdots, n)$且$a_i|m\ (i=1, 2, \cdots, n)\Longrightarrow a_1a_2\cdots a_n|m$.

12° $(a_i, b_j)=1\ (i=1, \cdots, n;\ j=1, \cdots, m)$

$$\Longrightarrow (a_1\cdots a_n, b_1\cdots b_m)=1$$

证明 由性质9°知道

$(a_1a_2\cdots a_n, b_j)=(a_2\cdots a_n, b_j)=\cdots=(a_n, b_j)=1$，$(j=1, 2, \cdots, m)$，再用性质9°得

$(a_1a_2\cdots a_n, b_1b_2\cdots b_m)=(a_1a_2\cdots a_n, b_2\cdots b_m)=\cdots=(a_1a_2\cdots a_n, b_m)=1$。

定义1·4 若 $a_i|m(i=1, 2, \cdots, n)$，则称整数m是非零整数 $a_1, a_2, \cdots, a_n$ 的公倍数（common multiple)。在 $a_1, a_2, \cdots, a_n$ 的一切公倍数中，最小的一个正整数叫做它们的最小公倍数（least common multiple)。记作

$$[a_1, a_2, \cdots, a_n]。$$

定理1·3 两正整数 a 和 b，必有

$$ab=(a, b)[a, b]。$$

证明 设 m' 是 a, b 的任一公倍数，由定义1·4知

$$m'=ak=bh$$

令 $a=a_1(a, b)$，$b=b_1(a, b)$，代入上式再消去(a, b)得

$$a_1k=b_1h$$

由定理1·2系2的(iii)知$(a_1, b_1)=1$，再由性质10°得 $b_1|k$，即 $k=b_1t$，所以

$$m'=ak=ab_1t=\frac{ab}{(a, b)}t,$$

即 a, b 的任一公倍数，都是 $\frac{ab}{(a, b)}$ 的倍数，并且 $ab/(a, b)$ 是 a, b 的公倍数，所以取 $t=1$ 时 $\frac{ab}{(a, b)}$ 是 a, b 的最小公倍数，

$$\therefore\ [a, b]=\frac{ab}{(a, b)}，即 (a, b)[a, b]=ab。$$

由定理1·3的证明过程中，已经得到

系1 二非0整数a和b的任何公倍数，都是$[a, b]$的倍数。

注意：定理1·3中二整数a和b必须同号，故设a，b为正整数是必要的，但系1里允许a，b异号，在证明过程中k，h，t可不限于正数。定理1·3不能推广于多于两个整数的情况。

系2 设n个非0整数$a_1, a_2, \cdots, a_n$，若$[a_1, a_2]=m_2$，$[m_2, a_3]=m_3$，…，$[m_{n-1}, a_n]=m_n$，
则

$$[a_1, a_2, \cdots, a_n]=m_n.$$

证明 从假设条件知

$m_i | m_{i+1} (i=1, 2, \cdots, n-1)$且$a_1 | m_2$，$a_i | m_i (i=2, \cdots, n) \Longrightarrow a_i | m_n (i=1, 2, \cdots, n)$，即$m_n$是$a_1, a_2, \cdots, a_n$的一个公倍数。

设m是$a_1, a_2, \cdots, a_n$的任一公倍数，则$a_1 | m$，$a_2 | m$，由定理1·3的系1得$m_2 | m$，又$a_3 | m \Longrightarrow m_3 | m$，又$a_4 | m \Longrightarrow m_4 | m$，…，$\Longrightarrow m_n | m \Longrightarrow m_n \leqslant |m|$，
由定义1·4知

$$[a_1, a_2, \cdots, a_n]=m_n.$$

从系2的证明中，已证明了

系3 n个非零整数$a_1, a_2, \cdots, a_n$，若$a_i | m (i=1, 2, \cdots, n)$，则$[a_1, a_2, \cdots, a_n] | m$。

例1·3 甲、乙两个齿轮，互相衔接，甲轮有437齿，乙轮有323齿，甲的某一齿与乙的某一齿从第一次接触到第二次接触，需要各转几周？

解 依题意，就是要先求出甲轮齿数和乙轮齿数的最小

公倍数。为此先用辗转相除法，求得

$$(437,\ 323)=19,$$

$$\therefore\quad [437,\ 323]=\frac{437\times 323}{19}=7429.$$

所以甲转　$7429\div 437=17$(周)

乙转　$7429\div 323=23$(周).

答：从甲的某一齿和乙的某一齿第一次接触后，甲转17周，乙转23周后才出现第二次接触。

第三节　辗转相除法与连分数

本节除从辗转相除法引入连分数的概念及研究其结构之外，还证明了任一实数都可表示为有限或无限连分数，及用连分数的渐近分数来作为实数的有理近似值是最佳的。

由第二节等式(2)我们有

$$\begin{cases} a=bq_1+r_2, \\ b=r_2q_2+r_3, \\ r_2=r_3q_3+r_4, \\ \cdots\quad\cdots\quad\cdots, \\ r_{n-3}=r_{n-2}q_{n-2}+r_{n-1} \\ r_{n-2}=r_{n-1}q_{n-1}+r_n \\ r_{n-1}=r_nq_n \end{cases} \Longrightarrow \begin{cases} \dfrac{a}{b}=q_1+\dfrac{r_2}{b}, \\ \dfrac{b}{r_2}=q_2+\dfrac{r_3}{r_2}, \\ \dfrac{r_2}{r_3}=q_3+\dfrac{r_4}{r_3}, \\ \cdots\quad\cdots\quad\cdots, \\ \dfrac{r_{n-3}}{r_{n-2}}=q_{n-2}+\dfrac{r_{n-1}}{r_{n-2}}, \\ \dfrac{r_{n-2}}{r_{n-1}}=q_{n-1}+\dfrac{r_n}{r_{n-1}}, \\ \dfrac{r_{n-1}}{r_n}=q_n. \end{cases} \tag{3}$$

$$\therefore\quad \frac{a}{b}=q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+\cfrac{\vdots}{+\cfrac{1}{q_{n-2}+\cfrac{1}{q_n}}}}} \tag{4}$$

形如(4)右边的分数，称为有限连分数，它可简写为

$$q_1+\frac{1}{q_2+}\ \frac{1}{q_3+}\cdots\frac{1}{q_{n-1}+}\ \frac{1}{q_n}\text{或}[q_1,\ q_2,\ \cdots,\ q_n]。$$

用后一种表示法时，必须注意它与最小公倍数的意义是不同的。

定义1·5 形如 $q_1+\frac{1}{q_2+}\ \frac{1}{q_3+}\cdots\frac{1}{q_n+}\cdots$的分数，叫做连分数(continued fraction)。令 $\delta_k=\frac{P_k}{Q_k}=q_1+\frac{1}{q_2+}\cdots\frac{1}{q_k}$，则称 δ_k 为该连分数的第 k 个渐近分数(k—th convegent)。

如，(4)的各渐近分数分别是：

$$\delta_1=\frac{P_1}{Q_1}=\frac{q_1}{1},\quad \delta_2=\frac{P_2}{Q_2}=q_1+\frac{1}{q_2}=\frac{q_2q_1+1}{q_2}$$

$$=\frac{q_2P_1+P_0}{q_2Q_1+Q_0},$$

其中$P_0=1$，$Q_0=0$。同样地，

$$\delta_3=\frac{P_3}{Q_3}=q_1+\cfrac{1}{q_2+\cfrac{1}{q_3}}=\frac{\left(q_2+\frac{1}{q_3}\right)P_1+P_0}{\left(q_2+\frac{1}{q_3}\right)Q_1+Q_0}$$

$$=\frac{q_3P_2+P_1}{q_3Q_2+Q_1}$$

等等．更普遍地

$$\delta_s=\frac{P_s}{Q_s}=\frac{q_sP_{s-1}+P_{s-2}}{q_sQ_{s-1}+Q_{s-2}}\quad(2\leqslant s\leqslant n).$$

今用数学归纳法证明如下：

证明　A）　当 $s=2$，3 时，显然结论成立。

B）　设小于 s 时结论成立．为 s 时有

$$\delta_s=\frac{P_s}{Q_s}=[q_1,q_2,\cdots,q_s]=[q_1,q_2,\cdots,q_{s-1}+\frac{1}{q_s}]$$

$$=\frac{(q_{s-1}+\frac{1}{q_s})P_{s-2}+P_{s-3}}{(q_{s-1}+\frac{1}{q_s})Q_{s-2}+Q_{s-3}}$$

$$=\frac{q_s(q_{s-1}P_{s-2}+P_{s-3})+P_{s-2}}{q_s(q_{s-1}Q_{s-2}+Q_{s-3})+Q_{s-2}}$$

$$=\frac{q_sP_{s-1}+P_{s-2}}{q_sQ_{s-1}+Q_{s-2}}.$$

从上面的分析，可得

定理1·4　若令 $P_0=1$，$Q_0=0$，$P_1=q_1$，$Q_1=1$，则连分数（4）的渐近分数 $\frac{P_s}{Q_s}$ 的分子和分母是

$$\begin{cases}P_s=q_sP_{s-1}+P_{s-2},\\Q_s=q_sQ_{s-1}+Q_{s-2}.\end{cases}\quad(s=2,3,\cdots,n)\qquad(5)$$

其计算方法可列表于下：

q_s		q_1	q_2	…	q_s	…	q_n
P_s	1	$P_1=q_1$	$P_2=1+q_1q_2$	…	$P_s=P_{s-2}+P_{s-1}q_s$	…	$P_n=a$
Q_s	0	$Q_1=1$	$Q_2=0+q_2$	…	$Q_s=Q_{s-2}+Q_{s-1}q_s$	…	$Q_n=b$

例如，由例1·2的演算知道

$$\frac{1859}{1573}=1+\frac{1}{5+}\frac{1}{2}.$$

q_s		$q_1=1$	$q_2=5$	$q_3=2$
P_s	1	1	6	13
Q_s	0	1	5	11

即$\delta_1=\frac{P_1}{Q_1}=1$，$\delta_2=\frac{P_2}{Q_2}=\frac{6}{5}$，$\delta_3=\frac{P_3}{Q_3}=\frac{2P_2+P_1}{2Q_2+Q_1}$

$$=\frac{13}{11}=\frac{1859}{1573}.$$

观察相邻两个渐近分数之差，有

$$\delta_s-\delta_{s-1}=\frac{P_s}{Q_s}-\frac{P_{s-1}}{Q_{s-1}}=\frac{P_sQ_{s-1}-P_{s-1}Q_s}{Q_sQ_{s-1}}$$

$$=\frac{h_s}{Q_sQ_{s-1}} \qquad (6)$$

系1 (6)中的$h_s=(-1)^s$，即$\delta_s-\delta_{s-1}$

$$=\frac{(-1)^s}{Q_sQ_{s-1}}.$$

证明 由(5)当$s=1$时，

$$h_1=P_1Q_0-Q_1P_0=q_1\times 0-1\times 1=-1=(-1)^1,$$

并且对于任意s都有

$$h_s=(q_sP_{s-1}+P_{s-2})Q_{s-1}-(q_sQ_{s-1}+Q_{s-2})P_{s-1}$$

$$=P_{s-2}Q_{s-1}-P_{s-1}Q_{s-2}=-h_{s-1}$$

$\therefore$ $h_2=-h_1=(-1)^2$，$h_3=-h_2=(-1)^3$，…，$h_s=(-1)^s$.

例如，上例中$\delta_2-\delta_1=\frac{6}{5}-1=\frac{1}{5}$，$\delta_3-\delta_2=\frac{13}{11}-$

$-\frac{6}{5}=-\frac{1}{55}$.

如有理数一样，我们也可以分解无理数成连分数，为此只须设法分出数 x 的整数部分[x]就可以了.

[x]是数论中的一个重要函数，它对一切实数都有意义，表示不大于 x 的最大整数，这函数叫做 x 的整数部分（integral part of x）. 并把 $x-[x]=\{x\}$ 叫做 x 的小数部分（decimal part of x）

例如，$[9]=9$，$[3.77]=3$，$[-3.77]=-4$；$\{9\}=0$，$\{3.77\}=0.77$，$\{-3.77\}=0.23$.

函数[x]和{x}有下列简单性质：

(i) $x=[x]+\{x\}$.

(ii) $[x]\leqslant x<[x]+1$；$x-1<[x]\leqslant x$；

$0\leqslant\{x\}<1$.

(iii) $[x]+[y]\leqslant[x+y]$；$\{x\}+\{y\}\geqslant\{x+y\}$.

证明 ∵ $[x]\leqslant x$，$[y]\leqslant y$，

∴ $[x]+[y]\leqslant x+y$

分别取整数部分，得

$$[[x]+[y]]=[x]+[y]\leqslant[x+y].$$

当 $\{x\}+\{y\}\geqslant 1$ 时，$\{x\}+\{y\}>\{x+y\}$；

当 $\{x\}+\{y\}<1$ 时，$\{x\}+\{y\}=\{x+y\}$，

∴ $\{x\}+\{y\}\geqslant\{x+y\}$.

(iv) $[n+x]=n+[x]$，n 是整数.

证明 ∵ $[n+x]=[n+[x]+\{x\}]=n+[x]$.

(v) $$[-x]=\begin{cases}-[x]-1, & \text{当 } x \text{ 不是整数时；}\\ -[x], & \text{当 } x \text{ 是整数时.}\end{cases}$$

证明 当 x 是整数时，显然

$$[-x]=-x=-[x];$$

当 x 不是整数时，$\{x\}>0$，$x=[x]+\{x\}$，

$\therefore\ [-x]=[-[x]-\{x\}]=[(-[x]-1)+(1-\{x\})]\overset{(iv)}{=}-[x]-1$.

(vi) 设 a，b>0 是两个整数，则

$$a=b\left[\frac{a}{b}\right]+b\left\{\frac{a}{b}\right\},\quad 0\leqslant b\left\{\frac{a}{b}\right\}\leqslant b-1.$$

证明 $a=\frac{ab}{b}=b\left(\left[\frac{a}{b}\right]+\left\{\frac{a}{b}\right\}\right)=b\left[\frac{a}{b}\right]+b\left\{\frac{a}{b}\right\}$,

又因 $b>0$，所以 $0\leqslant b\left\{\frac{a}{b}\right\}\leqslant b-1$.

事实上，(vi)的结论就是带余除法的结果，$a=bq+r$ 中，$q=\left[\frac{a}{b}\right]$，$r=b\left\{\frac{a}{b}\right\}$.

(vii) 若 a，b 是任意两个正整数，而不大于 a 而为 b 的倍数的数的个数是$\left[\frac{a}{b}\right]$.

证明 若 $a\leqslant b$ 显然成立. 若 $a>b$，m 是不大于 a 而为 b 的倍数的正整数，则 $0<m=bm_1\leqslant a$，即 $0<m_1\leqslant\frac{a}{b}$，故满足上述条件的 m 的个数，即满足 $0<m_1\leqslant\frac{a}{b}$的最大整数$m_1$，故$m_1=\left[\frac{a}{b}\right]$.

(viii) 在 n! 的标准分解式中，素因子 $p(p\leqslant n)$ 的指数

$$h=\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots=\sum_{r=1}^{\infty}\left[\frac{n}{p^r}\right].$$

注意：若 $p^s>n$，则$\left[\frac{n}{p^s}\right]=0$，故上式只有有限项不为0，因而有意义；并且 $p\leqslant n$ 的条件亦可删掉，因为 $p>n$ 时，$h=0$。

证明 设想把2，3，…，n 诸数都分解成标准分解式，则由算术基本定理（此定理将在第五节中证明之，这里先借用）知，h 就是这 $n-1$ 个分解式中 p 的指数之和，设其中 p 的指数是 $r(1\leqslant r)$的有 n_r 个，则

$$h=n_1+2n_2+3n_3+\cdots=(n_1+n_2+n_3+\cdots)+(n_2+n_3+\cdots)+(n_3+\cdots)=N_1+N_2+N_3+\cdots,$$

其中$N_r=n_r+n_{r+1}+\cdots$恰好是 $n-1$ 个数中能被 p^r 除尽的个数，由(vii)得$N_r=\left[\frac{n}{p^r}\right]$。

$$\therefore\quad h=\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots+\left[\frac{n}{p^r}\right]+\cdots=\sum_{r=1}^{\infty}\left[\frac{n}{p^r}\right].$$

由(viii)立即推得

系 1 $n!=\prod\limits_{p\leqslant n}p^{\sum\limits_{r=1}^{\infty}\left[\frac{n}{p^r}\right]}$，其中 $\prod\limits_{p\leqslant n}$ 表示不大于 n 的素数幂的连乘积。

系 2 贾宪数$\frac{m!}{k!(n-k)!}$是整数$(0<k<n)$。

证明 因为 $n=(n-k)+k$，由(iii)知$\left[\frac{n}{p^r}\right]\geqslant\left[\frac{n-k}{p^r}\right]+\left[\frac{k}{p^r}\right]$，于是$\sum\limits_{r=1}^{\infty}\left[\frac{n}{p^r}\right]\geqslant\sum\limits_{r=1}^{\infty}\left[\frac{n-k}{p^r}\right]+\sum\limits_{r=1}^{\infty}\left[\frac{k}{p^r}\right]$。

$$\therefore \prod_{p\leqslant n} p^{\sum\limits_{r=1}^{\infty}\left[\frac{n-k}{p^r}\right]+\sum\limits_{r=1}^{\infty}\left[\frac{k}{p^r}\right]} \Bigg| \prod_{p\leqslant n} p^{\sum\limits_{r=1}^{\infty}\left[\frac{n}{p^r}\right]}.$$

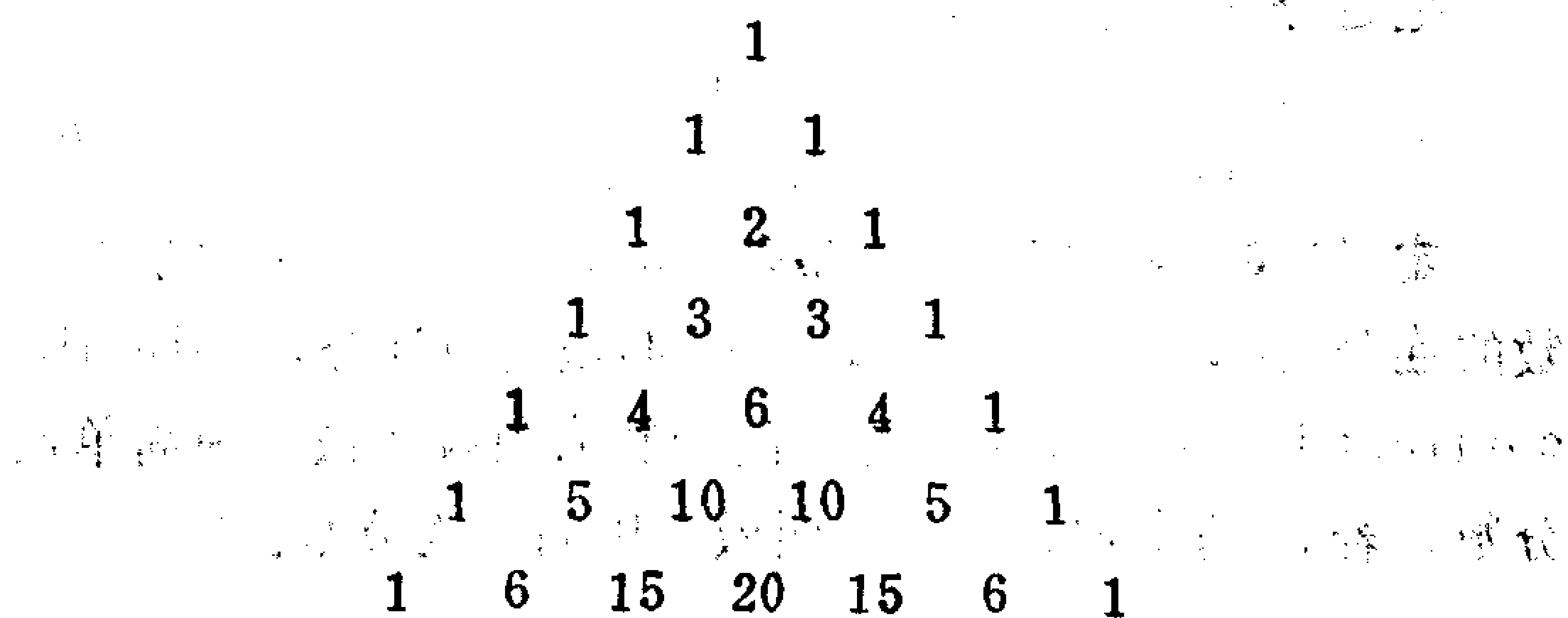
由系 1 知道 $k!(n-k)!\,\big|\,n!$，故贾宪数是整数。

系 2 给出了组合数 $C_n^r=\dfrac{n!}{r!(n-r)!}$一定是整数。由系2立即可得

系 3 若 $f(x)$是一个 n 次整系数多项式，$f^{(k)}(x)$ 是它的 k 阶导数($k\leqslant n$)，则$f^{(k)}(x)/k!$是一个 $n-k$ 次的整系数多项式。

其证明留给读者作练习。

$\dfrac{n!}{k!(n-k)!}$是二项式$(a+b)^n$的系数，这些数最先由我国数学家贾宪所发现，杨辉的著作《详解九章算法》(1261)里，指出贾宪已经用过下述的图形



因此我们可以看出二项式系数早在杨辉以前，即至迟在十三世纪已被我国人民所发现。这要比欧洲最早发现这个事实至少早260年左右，要比巴斯加（Pascal）发现此事实(1659)早400年。现在我国书中称上述图形为杨辉三角，实际上若称为贾宪三角更为确切。

例1·4 计算40！中出现3的方次数。

解： $h=\left[\frac{40}{3}\right]+\left[\frac{40}{9}\right]+\left[\frac{40}{27}\right]=13+4+1=18$。

要把实数α分解成连分数，首先应求得$[\alpha]=a_1$；$\alpha=a_1+\{\alpha\}$，$0<\{\alpha\}<1$。次令$\alpha_1=\frac{1}{\{\alpha\}}$，则

$$\alpha=a_1+\frac{1}{\alpha_1}, \quad \alpha_1>1;$$

$$\alpha_1=a_2+\frac{1}{\alpha_2}, \quad a_2=[\alpha_1], \quad \alpha_2=\frac{1}{\{\alpha_1\}}>1;$$

$$\cdots \quad \cdots \quad \cdots;$$

$$\alpha_{k-1}=a_k+\frac{1}{\alpha_k}, \quad a_k=[\alpha_{k-1}], \quad \alpha_k=\frac{1}{\{\alpha_{k-1}\}}>1;$$

$$\therefore \quad \alpha=a_1+\frac{1}{a_2+}\frac{1}{a_3+}\cdots\frac{1}{a_k+}\frac{1}{\alpha_k}=[a_1, a_2, a_3, \cdots, a_k, \alpha_k]. \tag{7}$$

把连分数化为分数，有

$$\alpha=\frac{\alpha_1 a_1+1}{\alpha_1}, \quad \alpha=\frac{\alpha_k P_k+P_{k-1}}{\alpha_k Q_k+Q_{k-1}} \quad (k=2, 3, \cdots). \tag{8}$$

定义1·6 我们把a_1是整数，a_2，…，a_k，…都是正整数的连分数$[a_1, a_2, \cdots, a_k, \cdots]$叫做简单连分数(simple continued fraction)。若a_i的个数有限就叫做有限简单连分数；若a_i的个数无限，就叫做无限简单连分数。对于无限简单连分数，我们仍用$\frac{P_k}{Q_k}=[a_1, a_2, \cdots, a_k]$，$(k=1, 2, \cdots)$，来表示它的第k个渐近分数。又如当$k\to\infty$时$\frac{P_k}{Q_k}$有一个极限，我们就把这个极限叫做该连分数的值(value)。

显然，定理1·4及系1，对于无限简单连分数的情况仍

然成立。定理1·4的

系 2 简单连分数的每一个渐近分数都是既约分数。

证明 ∵ $P_kQ_{k-1}-Q_kP_{k-1}=(-1)^k$

∴ $(P_k, Q_k)=1$.

事实上，否则有一个整数 $p>1$，使得 $p|P_k$ 且 $p|Q_k$，那末 $p|(-1)^k$，这是不可能的。

注意：本节前面所构造的连分数（即 $a_i=[\alpha_{i-1}]$）都是简单连分数，故以前的结论都适用于简单连分数。例如，

$$-\sqrt{2}=-2+(2-\sqrt{2})=-2+\cfrac{1}{\cfrac{1}{2-\sqrt{2}}}$$

$$=-2+\cfrac{1}{1+\cfrac{\sqrt{2}}{2}}=-2+\frac{1}{1+}\,\frac{1}{1+}\,\frac{1}{2+}\,\cfrac{1}{\cfrac{1}{\sqrt{2}-1}}$$

$=[-2, 1, 1, 2, 2, 2, \cdots]$是一个简单连分数。若

$$-\sqrt{2}=-1+(1-\sqrt{2})=-1+\cfrac{1}{\cfrac{1}{1-\sqrt{2}}}$$

$$=-1+\frac{1}{-2+(1-\sqrt{2})}$$

$$=-1+\cfrac{1}{-2+\cfrac{1}{\cfrac{1}{1-\sqrt{2}}}}$$

$$=[-1, -2, -2, -2, \cdots],$$

这就不是简单连分数了.

$$-\sqrt{2}=-3+(3-\sqrt{2})=-3+\cfrac{1}{\cfrac{3+\sqrt{2}}{7}}$$

$$= -3 + \cfrac{1}{0 + \cfrac{1}{\cfrac{7}{3+\sqrt{2}}}},$$

这是没有意义的，因为 0 不作为分母。

定理1·5 任一简单连分数都表示一个实数。

证明 显然，有限简单连分数都表示一个有理数，今设简单连分数

$$[a_1, a_2, \cdots, a_k, \cdots]$$

的渐近分数为

$$\frac{P_1}{Q_1}, \frac{P_2}{Q_2}, \cdots, \frac{P_k}{Q_k}, \cdots.$$

由定理1·4及其系 1，知

$$\frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}} = \frac{(-1)^k}{Q_k Q_{k-1}}$$

并且 $a_i \geqslant 1\ (i = 2, 3, \cdots)$，$Q_1 = 1$，$Q_2 = a_2 \geqslant 1$，$Q_3 = a_3 Q_2 + Q_1 = a_3 a_2 + 1 \geqslant 2$，$\cdots$，$Q_k = a_k Q_{k-1} + Q_{k-2} \geqslant k-1$。

$$\therefore \lim_{k\to\infty}\left|\frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}}\right| = \lim_{k\to\infty}\frac{|(-1)^k|}{Q_k Q_{k-1}}$$

$$\leqslant \lim_{k\to\infty}\frac{1}{(k-1)(k-2)} = 0 \qquad (9)$$

又因

$$\delta_{2k} - \delta_{2k-2} = \frac{P_{2k}}{Q_{2k}} - \frac{P_{2k-2}}{Q_{2k-2}} = \left(\frac{P_{2k}}{Q_{2k}} - \frac{P_{2k-1}}{Q_{2k-1}}\right) + \left(\frac{P_{2k-1}}{Q_{2k-1}} - \frac{P_{2k-2}}{Q_{2k-2}}\right)$$

$$= \frac{1}{Q_{2k}Q_{2k-1}} - \frac{1}{Q_{2k-1}Q_{2k-2}} = \frac{Q_{2k-2} - Q_{2k}}{Q_{2k}Q_{2k-1}Q_{2k-2}}$$

$$= \frac{Q_{2k-2} - a_{2k}Q_{2k-1} - Q_{2k-2}}{Q_{2k}Q_{2k-1}Q_{2k-2}} = \frac{-a_{2k}}{Q_{2k}Q_{2k-2}} < 0.$$

$$\therefore \quad \delta_{2k} < \delta_{2k-2} < \cdots < \delta_2 = a_1 + \frac{1}{a_2}.$$

同理

$$\delta_{2k-1} - \delta_{2k-3} = \frac{P_{2k-1}}{Q_{2k-1}} - \frac{P_{2k-3}}{Q_{2k-3}} = \frac{a_{2k-1}}{Q_{2k-1}Q_{2k-3}} > 0,$$

而 $\delta_{2k} - \delta_{2k-1} = \dfrac{(-1)^{2k}}{Q_{2k}Q_{2k-1}} > 0$，$\delta_{2k-1} - \delta_{2k-2} < 0$，

$$\therefore \quad \delta_{2k} > \delta_{2k-1} > \delta_{2k-3} > \cdots > \delta_1 = a_1.$$

且一切偶次渐近分数都大于奇次渐近分数。从而得到

$$\delta_2, \delta_4, \cdots, \delta_{2k} \tag{10}$$

是一个有界递减序列，其下界是 a_1；

$$\delta_1, \delta_3, \cdots, \delta_{2k-1} \tag{11}$$

是一个有界递增序列，其上界是$a_1 + \dfrac{1}{a_2}$。

因此$[\delta_{2k-1}, \delta_{2k}]$($k = 1, 2, \cdots$)作成一个区间套，故$\lim\limits_{k\to\infty} \delta_k$ 存在。

定理1·6 任一实无理数都可表成无限简单连分数，并且其表示法是唯一的。

证明 设 α 是实无理数，因为实无理数不能用分数来表示，所以(7)中的 α_k 仍是无理数，今证明

$$\lim_{k\to\infty} [a_1, a_2, \cdots, a_k] = \alpha. \tag{12}$$

由(8)式及(6)式得

$$\alpha - \frac{P_k}{Q_k} = \frac{\alpha_k P_k + P_{k-1}}{\alpha_k Q_k + Q_{k-1}} - \frac{P_k}{Q_k} = \frac{(-1)^{k-1}}{Q_k(\alpha_k Q_k + Q_{k-1})} \tag{13}$$

但是 $\alpha_k > a_{k+1} = [\alpha_k]$，故 $\alpha_k Q_k + Q_{k-1} > a_{k+1}Q_k + Q_{k-1} = Q_{k+1} \geqslant k$。

$$\therefore \quad \left|\alpha-\frac{P_k}{Q_k}\right|=\frac{1}{Q_k(\alpha_kQ_k+Q_{k-1})}\leqslant\frac{1}{k(k-1)},$$

当$k\to\infty$时，$\frac{1}{k(k-1)}\to 0$，故$\lim\limits_{k\to\infty}\frac{P_k}{Q_k}=\alpha$，即$\alpha$可表成无限简单连分数.

今证明其唯一性：若α可表成两个简单连分数

$$\alpha'=[a_1, a_2, \cdots, a_k, \cdots]$$

$$\beta'=[b_1, b_2, \cdots, b_k, \cdots]$$

当$\alpha'=\beta'=\alpha$时，由于α'与β'的整数部分相等，小数部分亦相等，简单连分数要求a_2、b_2是正整数，故只能是

$$a_1=[\alpha']=[\beta']=b_1,\ \text{且}\{\alpha'\}=\{\beta'\}$$

应用数学归纳法，假定$a_j=b_j$及$\alpha_j=\beta_j(j=1, \cdots, k)$

$$\therefore \quad \alpha'=[a_1, a_2, \cdots, a_k, \alpha_k]$$

$$\beta'=[b_1, b_2, \cdots, b_k, \beta_k]$$

$$=[a_1, a_2, \cdots, a_k, \beta_k]$$

这里必$\alpha_k=\beta_k>1$，简单连分数要求a_{k+1}，a_{k+2}，b_{k+1}，b_{k+2}都是正整数，故有

$$b_{k+1}=[\beta_k]=[\alpha_k]=a_{k+1},$$

且

$$\beta_{k+1}=\frac{1}{\{\beta_k\}}=\frac{1}{\beta_k-[\beta_k]}=\frac{1}{\alpha_k-[\alpha_k]}=\frac{1}{\{\alpha_k\}}$$

$$=\alpha_{k+1},$$

所以α的分解式是唯一的.

系 $\alpha=\frac{P_k}{Q_k}+\frac{(-1)^{k-1}\varepsilon_k}{Q_kQ_{k+1}}$或$\alpha=\frac{P_k}{Q_k}+\frac{(-1)^{k-1}\varepsilon_k'}{Q_k^2}$,

其中$0<\varepsilon_k<1$，$0<\varepsilon_k'<1$.

证明 因为$Q_{k+1}<\alpha_k$，所以$0<\frac{1}{\alpha_kQ_k+Q_{k-1}}<\frac{1}{Q_{k+1}}$

$<\frac{1}{Q_k}$，即存在$0<\varepsilon_k<1$，$0<\varepsilon_k'<1$的ε_k、ε_k'使得

$$\frac{1}{\alpha_k Q_k+Q_{k-1}}=\frac{\varepsilon_k}{Q_{k+1}}=\frac{\varepsilon_k'}{Q_k}$$

成立，把上式代入（13）的右边，移项后即得系中的结论。

这个系说明了，用α的第k个渐近分数作为α的有理近似值，其绝对误差小于$1/Q_kQ_{k+1}$，即

$$\left|\alpha-\frac{P_k}{Q_k}\right|<\frac{1}{Q_kQ_{k+1}}.$$

与定理1·6同样的方法，可以证明

定理1·7 对于有理数$\frac{a}{b}$

（i） 若$\frac{a}{b}=[a_1, a_2, \cdots, a_n]=[b_1, b_2, \cdots, b_m]$且$a_n>1$，$b_m>1$，则$m=n$，$a_i=b_i(i=1, 2, \cdots, n)$。

（ii） $\frac{a}{b}$有且仅有两种方法表成简单连分数，即

$$\frac{a}{b}=[a_1, a_2, \cdots, a_n]=[a_1, a_2, \cdots, a_n-1, 1]$$
$$(a_n>1)$$

定理1·8 若α是任一实数，$\frac{P_k}{Q_k}$是α的第k个渐近分数，则在分母$q\leqslant Q_k$的一切有理数中，$\frac{P_k}{Q_k}$是α的最好的有理近似值。即若$0<q\leqslant Q_k$，则

$$\left|\alpha-\frac{P_k}{Q_k}\right|\leqslant\left|\alpha-\frac{p}{q}\right| \qquad (14)$$

证明 若$\alpha=\frac{P_k}{Q_k}$，则定理已经成立，因此，只须讨论$\alpha\neq\frac{P_k}{Q_k}$的情形，此时存在$\alpha$的第$k+1$个渐近分数$\frac{P_{k+1}}{Q_{k+1}}$，

我们不妨假设$\frac{P_k}{Q_k}<\frac{P_{k+1}}{Q_{k+1}}$（若$\frac{P_{k+1}}{Q_{k+1}}<\frac{P_k}{Q_k}$可以同法讨论之）。

（i） 我们证明：若$0<q\leqslant Q_k$，则

$$\frac{p}{q}\leqslant\frac{P_k}{Q_k}\text{或}\frac{P_{k+1}}{Q_{k+1}}<\frac{p}{q},\qquad(\alpha)$$

否则，若$\frac{P_k}{Q_k}<\frac{p}{q}\leqslant\frac{P_{k+1}}{Q_{k+1}}$，由于$\frac{P_{k+1}}{Q_{k+1}}$是既约分数，且$q\leqslant Q_k<Q_{k+1}$，故$\frac{P_k}{Q_k}<\frac{p}{q}<\frac{P_{k+1}}{Q_{k+1}}$。因此

$$\frac{p}{q}-\frac{P_k}{Q_k}=\frac{pQ_k-P_kq}{qQ_k}\geqslant\frac{1}{qQ_k},\quad\frac{P_{k+1}}{Q_{k+1}}-\frac{p}{q}\geqslant\frac{1}{Q_{k+1}q}.$$

由于$Q_{k+1}+Q_k>q$，得

$$\frac{P_{k+1}}{Q_{k+1}}-\frac{P_k}{Q_k}=\left(\frac{P_{k+1}}{Q_{k+1}}-\frac{p}{q}\right)+\left(\frac{p}{q}-\frac{P_k}{Q_k}\right)\geqslant\frac{1}{qQ_{k+1}}+\frac{1}{qQ_k}=\frac{Q_{k+1}+Q_k}{qQ_kQ_{k+1}}>\frac{1}{Q_kQ_{k+1}},$$

这与定理1·4系1的结论矛盾，故（α）成立。

（ii） 由定理1·5证明的过程中及$\frac{P_k}{Q_k}<\frac{P_{k+1}}{Q_{k+1}}$，即得

$$\frac{P_k}{Q_k}<\alpha\leqslant\frac{P_{k+1}}{Q_{k+1}}$$

若$\frac{p}{q}\leqslant\frac{P_k}{Q_k}$，则（14）显然成立，若$\frac{P_{k+1}}{Q_{k+1}}<\frac{p}{q}$，则

$$\left|\alpha-\frac{p}{q}\right|\geqslant\left|\frac{P_{k+1}}{Q_{k+1}}-\frac{p}{q}\right|\geqslant\frac{1}{qQ_{k+1}}\geqslant\frac{1}{Q_kQ_{k+1}}.$$

另一方面，由定理1·6的系知道：$\left|\alpha-\frac{P_k}{Q_k}\right|<\frac{1}{Q_kQ_{k+1}}$，故得不等式（14）。

例如，用辗转相除法，可以算出

$$\frac{76501}{29719}=[2,1,1,2,1,6,1,4],$$

$$-\frac{48}{109}=[-1,1,1,3,1,2,4].$$

又 $1+\sqrt{5}=[3,4,4,4,\cdots]$，因此

	0	1	2	3	4	5	…
q_s		3	4	4	4	4	…
P_s	1	3	13	55	233	987	…
Q_s	0	1	4	17	72	305	…

$$\therefore\quad \left|\alpha-\frac{P_4}{Q_4}\right|=\left|1+\sqrt{5}-\frac{233}{72}\right|<\frac{1}{72\times305}<\frac{1}{10^4},$$

所以以$\frac{233}{72}$作为$1+\sqrt{5}$的近似就准确到小数点后四位了。

我国古代数学家柯承天（370～447）发现可以用$\frac{22}{7}$（约率）表示圆周率π的近似值，祖冲之（429—500）发现可以用$\frac{355}{113}$（密率）作为圆周率π的近似值，比西欧最早发现这一事实早1000年。实际计算我们知道π的连分数是：

$$\pi=[3,7,15,1,292,1,1,1,21,31,14,2,1,2,2,2,2,1,84,2,1,1,15,3,13,1,4,2,6,6,1,\cdots]$$

其渐近分数是：

$$\frac{3}{1},\ \frac{22}{7},\ \frac{333}{106},\ \frac{355}{113},\ \frac{103993}{33102},\ \frac{104348}{33215},\ \cdots,$$

而约率及密率刚好是π的两个渐近分数，由定理1·8知道，它们都是最佳近似值，由定理1·6的系知道

$$\left|\pi-\frac{355}{113}\right|<\frac{1}{113\times 33102}<\frac{1}{10^6},$$

故密率是 π 准确到小数点后六位的有理近似值，事实上，$\frac{355}{113}=3.1415929\cdots$. 由此可见，祖冲之在数学上的成就是惊人的，他确是世界上第一流的数学家。

下面将介绍循环连分数与二次根式的关系。

定义1·7 对于一个无限简单连分数 $[a_1,\cdots,a_n,\cdots]$ 若能找到两个整数 $s\geqslant 0$ 和 $t>0$ 使得

$a_{s+i}=a_{s+kt+i}$, $(i=1, 2, \cdots, t; k=1, 2, \cdots)$，我们就把这个无限简单连分数叫做循环连分数（periodic continued fraction）。并简记为

$$[a_1, \cdots, a_s, \dot{a}_{s+1}, \cdots, \dot{a}_{s+t}]$$

注意：若 $\alpha=[a_1, \cdots, a_n, \cdots]=[a_1, \cdots, a_s, \dot{a}_{s+1}, \cdots, \dot{a}_{s+t}]$ 是一个循环连分数，$\alpha_n=[a_{n+1}, a_{n+2}, \cdots]$，则 $\alpha_{s+i}=\alpha_{s+i+kt}$ $(k=0, 1, 2, \cdots)$，即

$$\begin{aligned}\alpha&=[a_1, a_2, \cdots, a_{s+i}, \alpha_{s+i}]\\&=[a_1, a_2, \cdots, a_{s+i+t}, \alpha_{s+i+t}]\\&=\cdots=[a_1, a_2, \cdots, a_{s+i+kt}, \alpha_{s+i+kt}]=\cdots\end{aligned}\qquad(15)$$

反之，若（15）成立，则 α 是一个循环连分数。

例如，$1+\sqrt{5}=[3, 4, 4, 4, \cdots]=[3, \dot{4}]$；

$\sqrt{28}=[5,\dot{3},2,3,\dot{10}]$，$\alpha_5=[3, 2, 3, 10, 3,\cdots]$ $=\alpha_9=\alpha_{13}=\alpha_{17}=\cdots$；$\alpha_6=[2, 3, 10, 3, 2, \cdots]=\alpha_{10}=\alpha_{14}=\cdots$

例1·5 将方程

$$x^4-x-1=0\qquad(a)$$

的正根分解成连分数。

解 容易看出，这个方程有且只有一个正根位于1与2之间，因此可以假设

$$x = 1 + \frac{1}{y}, \quad y > 1$$

为了把(a)的左边按$\frac{1}{y} = x - 1$的乘幂展开，应用高等代数上有名的和那（Horner）方法，这个方法是和那在1819年提出的，但我国宋朝刘益解二次方程时就用到了这种方法，他比和那早700多年，宋朝贾宪使用类似的方法亦比和那早600年，到宋秦九韶完整地发明了天元算法，亦比和那早500多年，其方法是用综合除法求出变形后方程的各项系数。如

```
1 + 0 + 0 - 1 - 1 | 1
    1 + 1 + 1 + 0
-------------------
1 + 1 + 1 + 0 | -1
  + 1 + 2 + 3
-------------------
1 + 2 + 3 | + 3
  + 1 + 3
-------------------
1 + 3 | + 6
  + 1
-------------------
1 | + 4
```

简写为

	1	0	0	−1	−1
1	1	1	1	0	−1
1	1	2	3	3	
1	1	3	6		
1	1	4			

$$\therefore \quad x^4 - x - 1 = \frac{1}{y^4} + 4\frac{1}{y^3} + 6\frac{1}{y^2} + 3\frac{1}{y} - 1 = 0$$

即 $y^4 - 3y^3 - 6y^2 - 4y - 1 = 0$ (b)

(b)的正根 $4 < y < 5$，因此，取$y = 4 + \frac{1}{z}$，即$\frac{1}{z} = y - 4$ $(z > 1)$。用和那法可求出

$$49z^4 - 60z^3 - 54z^2 - 13z - 1 = 0, \qquad \text{(c)}$$

这方程有正根 $1<z<2$，令 $z-1=\frac{1}{t}$（$t>0$），得

$$79t^4+105t^3-60t^2-136t-49=0, \qquad (d)$$

(d)的根 $1<t<2$，令 $t-1=\frac{1}{u}$，计算得

$$61u^4-375u^3-729u^2-421u-79=0 \qquad (e)$$

有正根 $6<u<7$，…。所以(a)的正根是

$$x=1+\frac{1}{4+}\,\frac{1}{1+}\,\frac{1}{1+}\,\frac{1}{6+}\cdots$$

$$=[1,\ 4,\ 1,\ 1,\ 6,\ \cdots].$$

若再演算下去，知道它不是循环连分数。

用连分数来计算代数方程根的近似值的方法是十八世纪拉格朗日所发明。

例1·6 将方程

$$2^x=5 \qquad (a)$$

的根分解成连分数。

解 显然(a)的根 $2<x<3$，令 $x=2+\frac{1}{y}$，（$y>1$），代入(a)得

$$2^{2+\frac{1}{y}}=4\cdot 2^{\frac{1}{y}}=5，\ 或\left(\frac{5}{4}\right)^y=2 \qquad (b)$$

由验算知道(b)的根 $3<y<4$，令 $y=3+\frac{1}{z}$（$z>1$）．代入(b)得

$$\left(\frac{5}{4}\right)^{3+\frac{1}{z}}=2\Longrightarrow\left(\frac{5}{4}\right)^{\frac{1}{z}}=\frac{128}{125}\Longrightarrow\left(\frac{128}{125}\right)^z=\frac{5}{4}$$

或 $(1.024)^z=1.25.$ (c)

经试验知(c)的根 $9<z<10$，…．

$$\therefore\quad x=\log_2 5=2+\frac{1}{3+}\,\frac{1}{9+}\cdots=[2,\ 3,\ 9,\ \cdots].$$

定理1·9 每一个循环连分数，都一定是某一个整系数二次不可约方程的实根。

证明 若循环连分数

$$\alpha=[a_1,\ \cdots,\ a_s,\dot{a}_{s+1},\ \cdots,\dot{a}_{s+t}],$$

令$\alpha_n=[a_{n+1},\ a_{n+2},\ \cdots]$。

当$s=0$时，由等式(8)得

$$\alpha=[\dot{a}_1,\ \cdots,\ \dot{a}_t]=[a_1,\ \cdots,\ a_t,\ \alpha]=\frac{\alpha P_t+P_{t-1}}{\alpha Q_t+Q_{t-1}}$$

$$\therefore \qquad Q_t\alpha^2+(Q_{t-1}-P_t)\alpha-P_{t-1}=0. \qquad (16)$$

若$s>0$，则由等式(8)及定义1·6下面的注意，得

$$\alpha=[a_1,\ \cdots,\ a_s,\ \alpha_s]=[a_1,\ \cdots,\ a_s,\ \cdots,\ a_{s+t},\ \alpha_s]$$

$$\Longrightarrow \alpha=\frac{\alpha_s P_s+P_{s-1}}{\alpha_s Q_s+Q_{s-1}}=\frac{\alpha_s P_{s+t}+P_{s+t-1}}{\alpha_s Q_{s+t}+Q_{s+t-1}}$$

$$\Longrightarrow \alpha_s=\frac{-Q_{s-1}\alpha+P_{s-1}}{Q_s\alpha-P_s}=\frac{-Q_{s+t-1}\alpha+P_{s+t-1}}{Q_{s+t}\alpha-P_{s+t}}$$

$$\Longrightarrow (Q_{s+t}\alpha-P_{s+t})(-Q_{s-1}\alpha+P_{s-1})=(Q_s\alpha-P_s)(-Q_{s+t-1}\alpha+P_{s+t-1})$$

即α是下列二次方程的实根：

$$(Q_{s+t}Q_{s-1}-Q_{s+t-1}Q_s)\alpha^2+(P_{s+t-1}Q_s+P_sQ_{s+t-1}-P_{s+t}Q_{s-1}-Q_{s+t}P_{s-1})\alpha+(P_{s+t}P_{s-1}-P_{s+t-1}P_s)=0 \qquad (16')$$

因为α是无限连分数，所以α不能是有理数（定理1·7），故α是无理数，(16)和(16′)都是二次不可约方程，并且(16)和(16′)的无理根一定是二次不尽根（二次根式）。

定理1·9的逆定理亦真。

定理1·10 若$f(x)=ax^2+bx+c$是一个整系数二次不可约多项式，α是$f(x)=0$的一个实根，则表示α的简单

连分数是一个循环连分数。

证明 因为 $f(x)$ 不可约，故 α 是无理数。由定理1·6知道，α 可表成一无限简单连分数，设 $\alpha_n=[a_{n+1}, a_{n+2},\cdots]$，则由等式(8)得

$$\alpha=\frac{\alpha_n P_n+P_{n-1}}{\alpha_n Q_n+Q_{n-1}},$$

代入 $f(x)$ 得

$$a\left(\frac{\alpha_n P_n+P_{n-1}}{\alpha_n Q_n+Q_{n-1}}\right)^2+b\left(\frac{\alpha_n P_n+P_{n-1}}{\alpha_n Q_n+Q_{n-1}}\right)+c=0$$

左边整理得到 α_n 的整系数方程

$$A_n\alpha_n^2+B_n\alpha_n+C_n=0$$

其中

$$\begin{cases}A_n=aP_n^2+bP_nQ_n+cQ_n^2,\\ B_n=2aP_nP_{n-1}+b(P_nQ_{n-1}+P_{n-1}Q_n)+2cQ_nQ_{n-1},\\ C_n=aP_{n-1}^2+bP_{n-1}Q_{n-1}+cQ_{n-1}^2=A_{n-1}.\end{cases}\quad(17)$$

故 α_n 是方程

$$A_ny^2+B_ny+C_n=0\qquad(18)$$

的一个实根，由(17)式及定理1·4系1，得

$$B_n^2-4A_nC_n=(b^2-4ac)(P_nQ_{n-1}-P_{n-1}Q_n)^2$$

$$=b^2-4ac.\qquad(19)$$

由定理1·6的系，得

$$P_n=\alpha Q_n+\frac{\varepsilon_n}{Q_n}(|\varepsilon_n|<1)$$

代入(17)的第一式，得

$$A_n=a\left(\alpha Q_n+\frac{\varepsilon_n}{Q_n}\right)^2+b\left(\alpha Q_n+\frac{\varepsilon_n}{Q_n}\right)Q_n+CQ_n^2$$

$$= (a\alpha^2 + b\alpha + c)Q_n^2 + 2a\alpha\varepsilon_n + a\frac{\varepsilon_n^2}{Q_n^2} + b\varepsilon_n$$

$$= 2a\alpha\varepsilon_n + a\frac{\varepsilon_n^2}{Q_n^2} + b\varepsilon_n,$$

$\therefore\quad |A_n| < |2a\alpha| + |a| + |b|.$

由(17)的第三式知，$C_n = A_{n-1}$，所以

$$|C_n| < |2a\alpha| + |a| + |b|.$$

最后，由(19)知

$$|B_n| \leqslant \sqrt{4|A_nC_n| + |b^2 - 4ac|} < \sqrt{4(2|a\alpha| + |a| + |b|)^2 + |b^2 - 4ac|}$$

由于a，b，c，α都是常数，故满足上面不等式的整数组(A_n, B_n, C_n)只能有有限个，因此在序列

$$(A_2, B_2, C_2), \cdots, (A_n, B_n, C_n), \cdots$$

中一定有三组值是相同的，即有三个正整数n_1，n_2，n_3 $(n_1 < n_2 < n_3)$存在，使得

$$A_{n1} = A_{n2} = A_{n3} = A,$$
$$B_{n1} = B_{n2} = B_{n3} = B,$$
$$C_{n1} = C_{n2} = C_{n3} = C.$$

由(18)知α_{n1}，α_{n2}，α_{n3}都是

$$Ay^2 + By + C = 0$$

的根，但f(x)不可约，故由(18)知$A_n \neq 0$（否则，α_n是有理数，于是$f(x) = 0$的根α也是有理数，这是不可能的），因而，上述方程有且只有二实根，所以α_{n1}，α_{n2}，α_{n3}中一定有两个相等，不妨设$\alpha_{n1} = \alpha_{n2}$。

α是实无理数，$\alpha_{n1} = \alpha_{n2}$也是实无理数，由定理1.6知

道只能唯一地表示为无限简单连分数，所以

$$a_{n_1+1}=a_{n_2+1},\quad a_{n_1+2}=a_{n_2+2},\quad \cdots.$$

令 $s=n_1$，$t=n_2-n_1$，即得

$$\alpha=[a_1, \cdots, a_s, \dot{a}_{s+1}, \cdots, \dot{a}_{s+t}].$$

第四节 欧拉括号

本节将介绍欧拉括号的概念及其性质，把它作为计算连分数的渐近分数及解不定方程的工具。

现在我们把辗转相除法推广如下：设 r 及 r_1 是所给的两数，而 k_1，k_2，…，k_n 是任何 n 个常数或变数（我们将把这些数看成正整数，但是下文所有代数上的结论，对于 r，r_1，k_1，…，k_n 为任意数时亦正确），现在我们从下列方程来探求数 r_2，r_3，…，r_n，r_{n+1}，…。

$$\begin{cases} r=k_1r_1+r_2, \\ r_1=k_2r_2+r_3, \\ \cdots\cdots\cdots, \\ r_{m-2}=k_{m-1}r_{m-1}+r_m, \\ r_{m-1}=k_mr_m+r_{m+1}, \\ r_m=k_{m+1}r_{m+1}+r_{m+2}, \\ \cdots\cdots\cdots, \\ r_{n-1}=k_nr_n+r_{n+1}. \end{cases} \tag{20}$$

(20)中的方程与(2)中的方程的区别在于：

(i) k_1k_2，…，k_n 并非用 r_1 除 r，r_2 除 r_1 等等所得的不完全商；而 q_1，q_2，…，q_n 都是用 b 除 a，r_2 除 b 等等所得的不完全商。

(ii) r_2，r_3，…，r_n，r_{n+1} 是由给定的 r，r_1 及 k_1

$(i=1, 2, \cdots, n)$根据(20)的欧拉算法(Euler's algorithm)来求得的；而(2)中的$q_i(i=1, \cdots, n)$和$r_i(i=2, \cdots, n)$都是由给定的a，b经欧几里德算法来求得的，所以欧几里德算法是欧拉算法的一种表示形式。

(iii) (20)的每一个方程都可以看作第一个，亦都可以看作最后一个；(2)就没有这个特点，并且(20)的r_i之值被相邻二式所唯一确定。如，把$r_m=k_{m+1}r_{m+1}+r_{m+2}$看作第一个方程，由此并可以求得$r_{m+2}, \cdots, r_n$的值，这里是把$r_m, r_{m+1}, k_i(i=1, \cdots, n)$作为已知的数，这样也可以向上递推，求得$r_{m-1}, \cdots, r_2, r_1, r$的值。例如，

$$r_{m+2}=r_m-k_{m+1}r_{m+1},$$

$$r_{m+3}=r_{m+1}-k_{m+2}r_{m+2}=r_{m+1}-k_{m+2}(r_m-k_{m+1}r_{m+1})$$

$$=-k_{m+2}r_m+(1+k_{m+1}k_{m+2})r_{m+1},$$

$$\cdots\cdots,$$

$$r_{m-1}=k_mr_m+r_{m+1},$$

$$r_{m-2}=k_{m-1}r_{m-1}+r_m=k_{m-1}(k_mr_m+r_{m+1})+r_m$$

$$=(k_{m-1}k_m+1)r_m+k_{m-1}r_{m+1},$$

$$\cdots\cdots.$$

所以r_i可由相邻二方程所唯一确定，依上面的演算方法，可以推得r用r_m，r_{m+1}表示的式子

$$r=Gr_m+Hr_{m+1}. \tag{21}$$

其系数G、H都是$k_1, k_2, \cdots, k_m$的整函数，其中G称为第一系数(first coefficient)，H称为第二系数(second coefficient)。(21)中若以r_m的表达式$k_{m+1}r_{m+1}+r_{m+2}$代入，则得r由r_{m+1}及r_{m+2}来决定的式子

$$r=(Gk_{m+1}+H)r_{m+1}+Gr_{m+2}. \tag{22}$$

比较(21)和(22)，得到一般的结论：

1．后式的第二系数等于前式的第一系数；

2．后式的第一系数等于前式的系数按表达式

$$Gk_{m+1}+H \tag{23}$$

来决定．

把$G=\{k_1, k_2, \cdots, k_m\}$叫做欧拉括号（Euler′bracket*），欧拉括号是$k_1, k_2, \cdots, k_m$的一个整函数．

欧拉算法及欧拉括号有下列诸性质。把(21)改写为

1° $$r=\{k_1, k_2, \cdots, k_m\}r_m+\{k_1, k_2, \cdots, k_{m-1}\}r_{m+1} \tag{21′}$$

由(21)、(23)得到系数的递推公式

2° $(G_0, H_0)=(G, H)\to(G_1, H_1)\to(G_2, H_2)\to\cdots$，其中$G_i=G_{i-1}k_{m+i}+H_{i-1}$，$H_i=G_{i-1}(i=1, 2, \cdots; G_{-1}=H_0)$，即

$$G_i=G_{i-1}k_{m+i}+G_{i-2}(i=1, 2, \cdots; G_{-1}=H_0) \tag{24}$$

用欧拉括号表示，就是

$$\{k_1, \cdots, k_{m+i}\}=\{k_1, \cdots, k_{m+i-1}\}k_{m+i}+\{k_1, \cdots, k_{m+i-2}\}. \tag{24′}$$

2°中当$i=1$，2时，$G_1=Gk_{m+1}+H$，$G_2=G_1k_{m+2}+G=(Gk_{m+1}+H)+G$，即

$$\begin{cases}\{k_1, \cdots, k_{m+1}\}=\{k_1, \cdots, k_m\}k_{m+1}\\ \qquad\qquad +\{k_1, \cdots, k_{m-1}\},\\ \{k_1, \cdots, k_{m+2}\}=\{k_1, \cdots, k_{m+1}\}k_{m+2}\\ \qquad\qquad +\{k_1, \cdots, k_m\}.\end{cases} \tag{24″}$$

我们只要知道了一元和二元的欧拉括号，就可以从公式

* 有的书中用$[k_1, k_2, \cdots, k_m]$来表示欧拉括号，我们为了避免与连分数的符号混乱，因而改用花括号（brace）代替方括号（bracket），把"bracket"改为"brace"为妥。这里保留原文。

(24′)依次算出多元的欧拉括号。由(20)的第1，2式知道：

$$r=(k_1k_2+1)r_2+k_1r_3$$

$$\therefore \quad \{k_1\}=k_1, \ \{k_1, \ k_2\}=k_1k_2+1 \qquad (25)$$

再由递推公式(24′)得

$$\{k_1, \ k_2, \ k_3\}=\{k_1, \ k_2\}k_3+\{k_1\}$$
$$=k_1k_2k_3+k_1+k_3,$$

由(21′)得

$$r=\{k_1, \ k_2, \ k_3\}r_3+\{k_1, \ k_2\}r_4$$
$$=(k_1k_2k_3+k_1+k_3)r_3+(k_1k_2+1)r_4,$$

连续推下去，得

$$\{k_1, \ k_2, \ k_3, k_4\}=k_1k_2k_3k_4+k_1k_2+k_1k_4+k_3k_4+1,$$

$r=(k_1k_2k_3k_4+k_1k_2+k_1k_4+k_3k_4+1)r_4+(k_1k_2k_3+k_1+k_3)r_5$，…等等，从递推公式(24)，当给定$k_1$，$k_2$，…，$k_m$时，可仿照连分数求渐近分数的方法，列表计算欧拉括号$\{k_1,\cdots,k_m\}$如下：

i		1	2	3	4	…	m
k_i		k_1	k_2	k_3	k_4	…	k_m
$G_i=G_{i-1}k_i+G_{i-2}$	$G_0=1$	$G_1=k_1$	$G_2=1+k_1k_2$	G_3	G_4	…	G_m

例如，计算{3，1，2，4，1，2}，若我们依次计算：{3}=3；{3，1}=3×1+1=4；{3，1，2}=4×2+3=11。{3，1，2，4}=11×4+4=48；{3，1，2，4，1}=48×1+11=59；{3，1，2，4，1，2}=59×2+48=166。

一般可简单地列表计算如下：

k_i		3	1	2	4	1	2
G_i	1	3	4	11	48	59	166

表中的 $G_i=\{k_1, \cdots, k_i\}=\{k_1, \cdots, k_{i-1}\}k_i+\{k_1, \cdots, k_{i-2}\}$ $(i>1)$

不用 r 而用 r_1，r_2 作为第一个数，与(21′)类似地得

$$\begin{cases} r_1=\{k_2, k_3, \cdots, k_m\}r_m+\{k_2, k_3, \cdots, \\ \qquad k_{m-1}\}r_{m+1}, \\ r_2=\{k_3, \cdots, k_m\}r_m+\{k_3, \cdots, k_{m-1}\}r_{m+1}. \end{cases} \tag{26}$$

把它们代入(20)的第一式，得

$$r=(k_1\{k_2, \cdots, k_m\}+\{k_3, \cdots, k_m\})r_m+ (k_1\{k_2, \cdots, k_{m-1}\}+\{k_3, \cdots, k_{m-1}\})r_{m+1}. \tag{27}$$

但是 r_m 及 r_{m+1} 可以看成独立变量，当 k_1，k_2，…，k_m 给定后，(20)的前m个方程就确定了，从而，把 r 表示成 r_m 及 r_{m+1} 的一次齐次函数只有唯一的形式，因此，比较(27)与(21′)，得与(24′)类似的

3° $$\{k_1, k_2, \cdots, k_m\}=k_1\{k_2, \cdots, k_m\}+\{k_3, \cdots, k_m\} \tag{28}$$

这个公式，使欧拉括号可以从“末尾”算起——先算 $\{k_m\}$，次 $\{k_{m-1}, k_m\}=k_{m-1}k_m+1$，继之，按公式(28)计算出的 $\{k_1, k_2, \cdots, k_m\}$，正如按(24′)计算 $\{k_m, k_{m-1}, \cdots, k_1\}$ 一样，从而得到下面重要的性质

4° $$\{k_1, \cdots, k_m\}=\{k_m, \cdots, k_1\}. \tag{29}$$

注意：等式(29)两道符号都是从右到左逐一计算的结果，并且公式(28)当m＝2时，没有意义，因为此时 $\{k_3,$

$\cdots, k_m\}$不存在，因此我们约定：当$m=2$时，$\{k_3, \cdots, k_m\}=\{\ \}$为"空"欧拉括号，并定义$\{\ \}=1$，这样就不必排除$m=2$的情况了，当$m=2$时，

$$\{k_1, k_2\}=k_1\{k_2\}+\{\ \}=k_1k_2+1$$

与(25)的结论一致。

性质4°前面的叙述确已证明了等式(29)，今再改用数学归纳法证明于下：

证明 A) $\because \{k_m\}=k_m$，

$$\{k_{m-1}, k_m\}=k_{m-1}\{k_m\}+\{\ \}=k_{m-1}k_m+1=$$
$$=k_m\{k_{m-1}\}+\{\ \}=\{k_m, k_{m-1}\}.$$

$$\{k_{m-2}, k_{m-1}, k_m\}=k_{m-2}\{k_{m-1}, k_m\}+\{k_m\}=$$
$$=k_{m-2}k_{m-1}k_m+k_{m-2}+k_m=$$
$$=k_m\{k_{m-1}, k_{m-2}\}+\{k_{m-2}\}$$
$$=\{k_m, k_{m-1}, k_{m-2}\}.$$

B) 设小于m个的欧拉括号，等式(29)都成立。如

$\{k_1, \cdots, k_{m-1}\}=\{k_{m-1}, \cdots, k_1\}$，$\{k_1, \cdots, k_{m-2}\}=\{k_{m-2}, \cdots, k_1\}$等等。则由(24″)及(28)得

$$\{k_1, \cdots, k_m\}=\{k_1, \cdots, k_{m-1}\}k_m+\{k_1, \cdots, k_{m-2}\}$$
$$=k_m\{k_{m-1}, \cdots, k_1\}+\{k_{m-2}, \cdots, k_1\}$$
$$=\{k_m, k_{m-1}, \cdots, k_1\}.$$

当我们把r_m，r_{m+1}看作(20)的第一式时，与(21′)相仿地，得

$$r_m=\{k_{m+1}, \cdots, k_n\}r_n+\{k_{m+1}, \cdots, k_{n-1}\}r_{n+1};$$
$$r_{m+1}=\{k_{m+2}, \cdots, k_n\}r_n+\{k_{m+2}, \cdots, k_{n-1}\}r_{n+1}.$$

代入(21′)得

$$r=(\{k_1, \cdots, k_m\}\{k_{m+1}, \cdots, k_n\}+\{k_1, \cdots, k_{m-1}\}\{k_{m+2}, \cdots, k_n\})r_n+(\{k_1, \cdots, k_m\}\{k_{m+1}, \cdots, k_{n-1}\}$$

$$+\{k_1,\cdots,k_{m-1}\}\{k_{m+2},\ \cdots,\ k_{n-1}\})r_{n+1}. \qquad (\alpha)$$

另一方面，在公式(21′)中取$m=n$，得

$$r=\{k_1,\ \cdots,\ k_n\}r_n+\{k_1,\ \cdots,\ k_{n-1}\}r_{n+1}. \qquad (\beta)$$

因为 r_n 和 r_{n+1} 是独立变量，故比较(α)和(β)中r_n的系数，得

5° $$\{k_1,\ \cdots,\ k_n\}=\{k_1,\ \cdots,\ k_m\}\{k_{m+1},\ \cdots,\ k_n\}+\{k_1,\ \cdots,\ k_{m-1}\}\{k_{m+2},\ \cdots,\ k_n\}. \qquad (30)$$

其中$1\leqslant m<n$。

当$m=1$时，(30)就是(28)，当$m=n-1$时，(30)就是(24″)的第一式，所以(30)是(24″)与(28)的推广，而(24″)与(28)是(30)的特例。

从(20)得

$$\begin{cases} r_{n+1}=-k_nr_n+r_{n-1}, \\ r_n=-k_{n-1}r_{n-1}+r_{n-2}, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots, \\ r_2=-k_1r_1+r \end{cases} \qquad (20')$$

(20′)与(20)形式上是相同的，仅仅是k_i的符号与(20)不同而已，因此，我们对欧拉括号的一切公式，若以$-k_i$代k_i，则对(20′)仍然成立。我们有：

$$\{-k_n\}=-k_n,$$

$$\{-k_n,\ -k_{n-1}\}=(-k_n)(-k_{n-1})+1=k_nk_{n-1}+1=\{k_nk_{n-1}\},$$

假设已证明$s\leqslant m$时，都有

$$\{-k_1,\ \cdots,\ -k_s\}=(-1)^s\{k_1\cdots,\ k_s\},$$

则由(24″)的第一式得

$$\{-k_1,-k_2,\cdots,-k_{m+1}\}=\{-k_1,\cdots,-k_m\}(-k_{m+1})$$

$$+\{-k_1, \cdots, -k_{m-1}\}=(-1)^{m+1}\{k_1,\cdots,k_m\}k_{m+1}$$
$$+(-1)^{m-1}\{k_1, \cdots, k_{m-1}\}$$
$$=(-1)^{m+1}\{k_1, \cdots, k_{m+1}\}.$$

从而得到，对任一正整数m，都有

6° $\{-k_1, \cdots, -k_m\}=(-1)^m\{k_1, \cdots, k_m\}$. (31)

现在我们从(20′)出发，按照公式(21′)可以用 r 和 r_1 的一次齐次式来表示 r_n：

$$r_n=\{-k_{n-1}, \cdots, -k_1\}r_1+\{-k_{n-1}, \cdots, -k_2\}r,$$

由性质6°及4°，得

7° $r_n=(-1)^{n-1}\{k_1, \cdots, k_{n-1}\}r_1+(-1)^n\{k_2, \cdots, k_{n-1}\}r$. (32)

把(21′)及(26)中的m改为n后，代入(32)中的 r 及 r_1，得

$$r_n=(-1)^{n-1}\{k_1, \cdots, k_{n-1}\}(\{k_2, \cdots, k_n\}r_n+\{k_2,\cdots, k_{n-1}\}r_{n+1})+(-1)^n\{k_2, \cdots,k_{n-1}\}(\{k_1, \cdots, k_n\}r_n+\{k_1, \cdots, k_{n-1}\}r_{n+1}).$$

$$\therefore\ (-1)^{n-1}\{k_1, \cdots, k_{n-1}\}\{k_2, \cdots, k_n\}+(-1)^n\{k_2, \cdots, k_{n-1}\}\{k_1,\cdots,k_n\}=1.$$

从而得到

8° $\{k_1, \cdots, k_n\}\{k_2, \cdots, k_{n-1}\}-\{k_1, \cdots, k_{n-1}\}\{k_2, \cdots, k_n\}=(-1)^n$. (33)

若 $k_1, k_2, \cdots, k_n$ 全是正整数，则容易得到欧拉括号 $\{k_1, \cdots, k_n\}$ 也是正整数，并且

$$\{k_1, \cdots, k_m\}>\{k_2,\cdots,k_m\}>\{k_3, \cdots, k_m\}>\cdots. \quad (m\leqslant n) \qquad (34)$$

当 $m=n$ 时，由(28)知道，k_1 是以 $\{k_2, \cdots, k_n\}$ 除 $\{k_1, \cdots, k_n\}$ 所得的不完全商，而 $\{k_3, \cdots, k_n\}$ 是余数；余

类推。因此，带余除法的等式(2)中，取$a=r$，$b=r_1$，$q_i=k_i(i=1,2,\cdots,n)$，则(3)可改写为

$$\frac{\{k_1,\cdots,k_n\}}{\{k_2,\cdots,k_n\}}=k_1+\frac{\{k_3,\cdots,k_n\}}{\{k_2,\cdots,k_n\}}$$

$$=k_1+\cfrac{1}{\cfrac{\{k_2,\cdots,k_n\}}{\{k_3,\cdots,k_n\}}},$$

同样地有

$$\frac{\{k_2,\cdots,k_n\}}{\{k_3,\cdots,k_n\}}=k_2+\cfrac{1}{\cfrac{\{k_3,\cdots,k_n\}}{\{k_4,\cdots,k_n\}}},$$

依此类推，可用欧拉括号的公式来化有理数$\frac{a}{b}$为连分数，可得与(4)同样的结果

$$\frac{a}{b}=\frac{\{k_1,k_2,\cdots,k_n\}}{\{k_2,k_3,\cdots,k_n\}}=k_1+\frac{1}{k_2+}\ \frac{1}{k_3+}\cdots\frac{1}{k_n}$$

$$=[k_1,k_2,\cdots,k_n]. \tag{35}$$

注意：这里的a，b是随给定的$k_1,\cdots,k_n$而确定的，由不等式(34)当$m=n$时，保证了$r_1>r_2>\cdots>r_n$。

定理1·11 欧拉算法的等式(20)中，若$k_1,\cdots,k_n$是任意的n个正整数，则可把它们看作是欧几里德算法应用到二正整数$a=r=\{k_1,\cdots,k_n\}$及$b=r_1=\{k_2,\cdots,k_n\}$的不完全商。并且可以把$\frac{a}{b}$化成连分数(35)。

从(2)和(32)知道，$r_n=(a,b)$，$r=a$，$r=b$，又可得

定理1·12 任意二正整数a和b，存在二整数s和t，使得

$$as+bt=(a,b). \tag{36}$$

特别，当a和b互素时，

$$as+bt=1. \tag{37}$$

事实上，$t=(-1)^{n-1}\{q_1,\cdots,q_{n-1}\}$，$s=(-1)^n\{q_2,\cdots,q_{n-1}\}$，这里假设 $a>b$，使$q_1>0$。

这个定理在整除性理论中是十分重要的。

例1·7 根据等式(29)，按相反方向计算

(i) $[3,5,1,1,2]$；

(ii) $\frac{1}{2+}\ \frac{1}{2+}\ \frac{1}{3+}\ \frac{1}{4}$.

解：(i) ∵ $\{3,5,1,1,2\}=\{2,1,1,5,3\}$

$$\begin{array}{cccccc} & 2 & 1 & 1 & 5 & 3 \\ \hline 1 & 2 & 3 & 5 & 28 & 89 \end{array},$$

所得的最后一个数，就是该分数的分子，倒数第二个数就是该分数的分母。

$$\therefore\quad [3,5,1,1,2]=\frac{89}{28}.$$

实际上，$89=\{2,1,1,5,3\}=\{3,5,1,1,2\}$；

$28=\{2,1,1,5\}=\{5,1,1,2\}$.

由等式(35)知道：

$$\frac{a}{b}=[3,5,1,1,2]=\frac{\{k_1,\cdots,k_5\}}{\{k_2,\cdots,k_5\}}=\frac{89}{28}.$$

注意：如果用“顺”的方向计算

$$\begin{array}{cccccc} & 3 & 5 & 1 & 1 & 2 \\ \hline 1 & 3 & 16 & 19 & 35 & 89 \end{array},$$

$35=\{3,5,1,1\}$就不是该分数的分母了。

(ii) $$\begin{array}{cccccc} & 4 & 3 & 2 & 2 & 0 \\ \hline 1 & 4 & 13 & 30 & 73 & 30 \end{array},$$

$$\therefore\quad \frac{1}{2+}\ \frac{1}{2+}\ \frac{1}{3+}\ \frac{1}{4}=\frac{30}{73}(=[0,2,2,3,4]).$$

由这个例子，可以得到用欧拉括号来简化连分数化分数及求渐近分数的计算。又如

$$\frac{\{q_1, \cdots, q_m\}}{\{q_2, \cdots, q_m\}} = [q_1, \cdots, q_m] \tag{38}$$

是(35)的第 m 个渐近分数，如，由下表

q_s		3	5	1	1	2
P_s	1	3	16	19	35	89
Q_s		1	5	6	11	28

给出了〔3,5,1，1,2〕的诸渐近分数：$\frac{P_1}{Q_1}=\frac{3}{1}$，$\frac{P_2}{Q_2}=\frac{16}{5}$，$\frac{P_3}{Q_3}=\frac{19}{6}$，$\frac{P_4}{Q_4}=\frac{35}{11}$，$\frac{P_5}{Q_5}=\frac{89}{28}=[3, 5, 1, 1, 2]$。

例1·8 上例(i)中 $(89, 28)=1$，求两整数 s 和 t，使 $89s+28t=1$。

解：因为$\frac{89}{28}=[3, 5, 1, 1, 2]$，由定理1·12知道

$s=(-1)^5\{5, 1, 1\}=-11$，$t=(-1)^4\{3, 5, 1, 1\}=35$。

∴ $89\times(-11)+28\times35=1$。

例1·9 已知$\sqrt{28}=[5, \dot{3}, 2, 3, \dot{10}]$，求$\sqrt{28}$准确到0.0001的近似值

q_s		5	3	2	3	10	3	2	…
P_s	1	5	16	37	127	1307	4048	…	
Q_s		1	3	7	24	247	765	…	

因为$247^2>10000$（或$247\times765>10000$），所以$\frac{P_5}{Q_5}=\frac{1307}{247}$是$\sqrt{28}$准确到0.0001的不足近似值。而经四舍五入得$\frac{1307}{247}\approx 5.2915$时却不知它是过剩还是不足的近似值。

定理1·13 任何形如$4s+1$的素数，都可以表成两个整数的平方和。

证明 设$p=4s+1$是素数，分数

$$\frac{p}{2},\ \frac{p}{3},\ \cdots,\ \frac{p}{2s} \tag{α}$$

都是大于2的既约分数，其分母$q=2,3,\cdots,2s$，今把它们分解成连分数

$$\frac{p}{q}=[k_1,\cdots,k_n]=\frac{\{k_1,\ \cdots,\ k_n\}}{\{k_2,\ \cdots,\ k_n\}} \tag{β}$$

其中$k_1\geqslant 2$，$n>1$，$k_n>1$。由于p/q和它的任一渐近分数都是不可约的，

$$\therefore\quad p=\{k_1,\ \cdots,\ k_n\},\ q=\{k_2,\ \cdots,\ k_n\}. \tag{γ}$$

反之，用任何方法（如，(20)式的方法）找到的用欧拉括号表示p的式子

$$p=\{k_1,\ \cdots,\ k_n\},\ k_1\geqslant 2,\ n>1,\ k_n>1 \tag{δ}$$

若把它写成连分数

$$[k_1,\cdots,k_n]=\frac{p}{q}>2,$$

则$q=\{k_2,\ \cdots,\ k_n\}<\frac{p}{2}$，也就是q只能是2，3，…，2s中的一个数。由性质4°又有

$$p=\{k_n,\ \cdots,\ k_1\},\ k_n\geqslant 2,\ n>1,\ k_1\geqslant 2 \tag{δ'}$$

$\frac{p}{q'}=[k_n,\ \cdots,\ k_1]$；$q'=\{k_{n-1},\ \cdots,\ k_1\}<\frac{p}{2}$亦是2，3，…，2s中的一个数。

这样一来，当 p 表示为一个欧拉括号(δ)时，在(α)中就产生分母为 q 和 q′ 的一对分数和它对应，把这样的一对分数记作(q，q′)，由于(α)中分数的个数2s－1是奇数，因此必然出现 q＝q′ 的一个分数对

$$\frac{p}{q}=\frac{\{k_1, \cdots, k_n\}}{\{k_2, \cdots, k_n\}}=\frac{p}{q'}=\frac{\{k_n, \cdots, k_1\}}{\{k_{n-1}, \cdots, k_1\}}$$

由于实数的连分数表示法是唯一的，它们对应的渐近分数都相等，故

$$k_1=k_n,\ k_2=k_{n-1},\ k_3=k_{n-2},\ \cdots$$

下面证明，n 一定是偶数，否则，若 $n=2m+1$ 为奇数，则

$$p=\{k_1, \cdots, k_m, k_{m+1}, k_m, \cdots, k_1\} \xlongequal{5^\circ} \{k_1, \cdots, k_m\}\cdot\{k_{m+1}, \cdots, k_1\}+\{k_1, \cdots, k_{m-1}\}\{k_m, \cdots, k_1\} \xlongequal{4^\circ}$$

$$=\{k_1, \cdots, k_m\}(\{k_1, \cdots, k_{m+1}\}+\{k_1, \cdots, k_{m-1}\})$$

其中每一个因子都大于1，这与 p 是素数的假设矛盾，故 n 是偶数。设 $n=2m$，由性质5°，4°立即得到

$$p=\{k_1, \cdots, k_m, k_m, \cdots, k_1\}=\{k_1, \cdots, k_m\}\{k_m, \cdots, k_1\}+\{k_1, \cdots, k_{m-1}\}\{k_{m-1}, \cdots, k_1\}=\{k_1, \cdots, k_m\}^2+\{k_1, \cdots, k_{m-1}\}^2.$$

这个分解式还是唯一的，其证法放在第七章。

例1·10 把73分解成两个整数的平方和。

解：$73=4\times18+1$ 是 $4s+1$ 形的素数，当 $q=27$ 时，我们有

$$\frac{73}{27}=[2, 1, 2, 2, 1, 2], \quad 73=\{2, 1, 2\}^2+\{2, 1\}^2=8^2+3^2.$$

最后举一些连分数应用的例子.

1. 齿轮 若要用齿轮来联系两个转轴，使它们角速度的比值等于所给的数 α，因为两齿轮的速度和齿数成反比例；故齿数的反比等于 α，然而 α 可能是无理数，而齿数总是不十分大的整数，因此，我们的问题只可能有近似的解，就是去取分母不十分大的分数作为 α 的近似值，最好的是取 α 的连分数的渐近分数为近似值（定理1·8）. 如，$\alpha=\sqrt{28}$，取 $\alpha=\frac{127}{24}$ 就是 $\sqrt{28}$ 准确到0.0002的近似值，也就是甲齿轮的齿数为24，乙齿轮的齿数为127，用它们来联系两个轴，则其转速之比，十分接近于 $\sqrt{28}$.

2. 历法 从天文学知道：一年有365.24220…个“平均”日，这样计算是不方便的，必须用更简单的数来表示，又要求尽可能地准确些，因此把它分解成连分数，

$$365.24220\cdots=365+\frac{1}{4+}\frac{1}{7+}\frac{1}{1+}\frac{1}{3+}\cdots$$

它的前面几个渐近分数是

$$365,\ 365\frac{1}{4},\ 365\frac{7}{29},\ 365\frac{8}{33},\ \cdots.$$

近似值 $365\frac{1}{4}$ 是古代中国人、埃及人、巴比伦人所早已知道的，如，中国淮南子天训：“反复三百六十五度四分度之一而成一岁. …日行一度而岁有奇四分度之一，故四岁而积千四百六十一日，而复合故舍，八十岁而复合故度”.（度当作日，一年 $365\frac{1}{4}$ 日，四年应增加一日，但这是过剩近似值，其过剩之数小于 $\frac{1}{4}-\frac{7}{29}=\frac{1}{116}$，约八十年差了一日.）当时还没闰年的规定，公元前238年3月7日多禄某·爱伐盖特的卡诺补法令颁发后，即以第四年改为366日，但

只实行40年，而被遗忘，直到公元前47年儒略·凯撒才在索西泽尼的参与下重复前制，每逢第四年的二月份增加一天，这一天叫做闰日(bissextile day)，这就是闰年的由来.这种历法称为旧历，亦称儒略（Julian）历。

新历也称格里历，即以近似值$365\frac{97}{400}$为岁实（平均太阳年），这个值比$365\frac{7}{29}$及$365\frac{8}{33}$更为准确（因$\frac{8}{33}>\frac{97}{400}>\frac{7}{29}$）. 它与儒略历的区别，在于每逢百数之年，不被400除尽者均不置闰。例如，1700、1800、1900年都不闰，1600、2000年都是闰年。也就是每400年添进97天而不是100天。

儒略历使用到十五世纪，就引起人们的注意，那时已差了十天，西欧直到十六世纪末才开始改革，凭罗马教皇格里高里十三世1582年3月1日的一纸诏书，把10月5日至14日一笔勾掉，而将1582年10月5日公认为10月15日。

其实，我国元朝至元十三年（1276年），郭守敬和其他历法家，参考历代历法，测候日月星辰运行的变动，分别异同，酌量采取中数，作出历法的根本. 又造仪器二十二种，设四方测站二十七处，昼夜密测，并创垛叠招差勾股弧矢等方法精密推算，而有授时历的制定，自1281年即行使用. 按授时历即以365.2425为岁实和格里高里历的岁实完全一样，却更早了300年.)明洪武元年至崇祯末年(1368—1644)所用的大统历基本上也就是授时历。)

1079年波斯的天文学家兼数学家(也是诗人)奥玛尔·阿勒海雅密提出的历书，规定33年为一次循环，每33年七次置闰于每第四年，而第八次置闰于第五年，而不是第四年，即平均每年$365\frac{8}{33}$，这个天数就是第四个渐近分数。

其它在不定方程和素数理论上的应用，将结合在以后章节里来介绍。

第五节　素数和算术基本定理

本节主要介绍算术基本定理并举些例子联系中学生数学竞赛. 本节所指的数都是正整数.

1 只有一个因数就是 1 本身，任何大于 1 的数 a，至少有 1 和 a 两个因数，例如，3 有且只有 1 和 3 两个因数；6 却有 1，2，3，6 四个因数. 以后把 1 和 a 叫做 a 的当然因数（natural factor）. $b|a$ 且 $1<b<a$ 的 b 叫做 a 的非当然因数或真因数（true factor）.

定义1·8　一个大于 1 的整数中，只有当然因数时，则称 p 为素数（prime），不是 1 和素数的正整数，称为复合数（composite number）简称合数（composite）.

从上面定义知，一切正整数可分为 1，素数和合数三类. 例如，2，3，5，7，11，…是素数，4，6，8，9，10，…是合数. 以后用 p，p_1，p_2，…，p_n，…等表示素数，用 a，b，c，…，m，n，…等表示合数.

定理1·14　有无限多个素数.

证明　用反证法，若素数的个数只有有限个，设为 p_1、p_2，…，p_n，则令

$$a=p_1p_2\cdots p_n+1.$$

若在 p_1，p_2，…，p_n 中有一个 $p_i|a$，则 $p_i|1$，这与 p_i 是素数的假设矛盾，所以 p_1，p_2，…，p_n 都不整除 a，因而 a 本身是素数，或者有一个素数 p，$p|a$ 且 $p\neq p_i\ (i=1,2,\cdots,n)$，这就说明了除这 n 个素数之外还有其它素数 p（或 a）存在，所以素数的个数是无穷的.

这个定理的上述证法，是早在公元前300年由欧几里德所给出。到十八世纪欧拉又用解析方法证明如下：

证明 设 p_i 是素数，我们有

$$\frac{1}{1-\frac{1}{p_i}}=\left(1-\frac{1}{p_i}\right)^{-1}=1+\frac{1}{p_i}+\frac{1}{p_i^2}+\cdots$$

$$=\sum_{k=0}^{\infty}\frac{1}{p_i^k} \tag{a}$$

级数(a)是公比为 $\frac{1}{p_i}<1$ 的正项等比级数，所以它是收敛的。

假设 p_1，p_2，…，p_n 是全部素数（n 是有限整数），那末取 $i=1, 2, \cdots, n$，由(a)得到 n 个收敛级数，把这 n 个等式的左右边分别连乘，根据无穷级数论的定理，有限个正项收敛级数的乘积的求法，与求有限和的乘积一样，用每个因式的每一项去乘其余每一个因式的每一项，所得的新级数也是收敛的正项级数。因为这些数的加、乘是可交换的，所以与乘积的项的顺序无关，乘积后级数的一般项是

$$\frac{1}{p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}}, \tag{b}$$

这里 α_1，α_2，…，α_n 是任意的非负整数。

既然我们认为素数有且只有 n 个：p_1，p_2，…，p_n，那末任何正整数都可以表成 $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$ 的形式，并且这种表示法是唯一的（算术基本定理，此定理本节后面将证明），所以(b)可以写成 $\frac{1}{m}$ 的形式，m 是任意正整数。因此 n 个级数(a)的乘积等于

$$\sum_{m=1}^{\infty}\frac{1}{m}$$

是一个调和级数，它是发散的，这与前面所得收敛的结论矛盾。得到这个矛盾的原因是因为我们假定素数的个数是有限的（n 个），所以素数的个数是无限的。

素数的理论是丰富多采的，历史上许多数学家致力于研究素数的分布情况，并企图用一个公式来表示素数，就是求得变数 x 的一个函数，使它当 x 取任何正整数或非负整数时，该函数的值都是素数（不一定包括一切素数）。欧拉曾构造过

$$f(x)=x^2+x+41,$$

当 $x=0, 1, \cdots, 39$ 时，$f(x)$ 都是素数，而 $x=40$ 时 $f(40)=41^2$。类似地，$g(x)=x^2+x+17$，当 $x=0, 1, \cdots, 15$ 时，$g(x)$ 都是素数，当 $x=16$ 时，$g(16)=17^2$ 为合数，$h(x)=2x^2-29$，当 $x=0, 1, \cdots, 28$ 时，$h(x)$ 是素数，而 $f(29)=29\times59$ 为合数。

近代毕佳尔（Beeger）算出

$$k(x)=x^2-x+72491,$$

当 $0\leqslant x\leqslant 11000$ 时都是素数，因而提出一个猜测：任给一个正整数N，都可找出一个素数 p，当 $0\leqslant n\leqslant N$ 时，使

$$n^2-n+p \tag{39}$$

都是素数。我国数学家华罗庚认为要证明这个猜测比证明哥德巴赫猜想更难。

若上面猜想已被证实，就可以证明 $p'-p=2$ 的素数对 p、p′（孪生素数 prime twins）是无穷的（这个问题第八章将作简单介绍）。事实上，多项式（39）最多只能当 n

由 0 至 $p-1$ 时为素数，因而当 $N_1>p$ 时，仍存在 $p_1>N_1$ 使得当 $0\leqslant n\leqslant N_1$ 时

$$n^2-n+p_1$$

都是素数，取 $n=1,2$ 时，则 p_1，p_1+2 就是距离为2的素数对，取 $N_2>p_1$，则存在 $p_2>p_1$ 使得当 $0\leqslant n\leqslant N_2$ 时

$$n^2-n+p_2$$

都是素数，故有孪生素数 p_2，p_2+2，依此类推可得无穷多对孪生素数。

历史上，要找一个定义在整数集里的多项式函数，使其值域是素数集的企图都失败了。一般地

定理1·15 任何一个整系数的次数大于0的多项式函数 $f(x)$，总不可能对于 x 取任何自然数 a 时，$f(a)$ 都是素数。

证明 用反证法，若存在整系数多项式

$$f(x)=a_0x^m+a_1x^{m-1}+\cdots+a_m\ (a_0\neq 0,\ m>0).$$

使得当 $x=a$ 为任意自然数时，$f(x)=f(a)=\pm p$（p 是素数），则研究

$$f(a+py)-f(a)=a_0[(a+py)^m-a^m]+a_1[(a+py)^{m-1}-a^{m-1}]+\cdots+a_{m-1}py,$$

$$\therefore\quad f(a+py)=f(a)+a_0[(a+py)^m-a^m]+a_1[(a+py)^{m-1}-a^{m-1}]+\cdots+a_{m-1}py.$$

p 整除上式右边的每一项，由整除的性质3°知，$p\mid f(a+py)$，其中 y 可以取任何自然数。由假设当 $x=a+py$ 时，$f(a+py)$ 是素数，并且 p 整除这个素数，所以 $f(a+py)=\pm p$。

$$\therefore\quad [f(a+py)]^2-[f(a)]^2=p^2-p^2=0,$$

即 $[f(a+py)-f(a)]\cdot[f(a+py)+f(a)]=0$ 中必有一个因式对于 y 为一切自然数时都等于0，但 $y=0$ 时，

$f(a+p\cdot 0)=f(a)$，又 $f(a+py)$ 是 y 的 m 次多项式，故有

$$f(a+py)\equiv f(a)$$

为常数，也就是有无穷多个的 x 的值（$x=a+py$，y 取任意值），使得 $f(x)=f(a)$，所以 $f(x)=f(a)=\pm p$ 为常数，这与 $f(x)$ 是 $m(>0)$ 次多项式的假设矛盾。

历史上，许多数学家企图用 x 的非有理函数来表示素数。我们容易证明

定理1·16 若 $a\geqslant 2$ 且 a^n+1 是素数，则 a 是偶数且 $n=2^m$。

证明 若 a 是奇数，则 a^n+1 是偶数，当 $n>0$ 时，a^n+1 都是大于 2 的偶数，故为合数，所以 a 必为偶数。

其次，若 n 有奇数因子 $k(\geqslant 3)$，则 $n=kl$，因而 $a^l+1|a^n+1$ 且

$$\frac{a^{kl}+1}{a^l+1}=a^{(k-1)l}-a^{(k-2)l}+\cdots+1$$

其中 $a^l+1\geqslant 3$，故 a^n+1 是合数。

定理1·17 若 $n>1$ 且 a^n-1 是素数，则 $a=2$ 且 n 是素数。

证明 若 $a>2$，则 $a-1|a^n-1$；若 $a=2$ 且 $n=kl$ 为合数，则 $2^k-1|2^n-1$。

这两个定理给出了指数函数为素数的某种必要条件，但非充分的，为此默森尼(Mersenne)研究了形如 2^p-1 的素数，其中 p 是素数，他在1644年证明了 $M_p=2^p-1$ 是素数的有

$p=2$，3，5，7，13、17、19、31、67、127、257。

并证小于257的其他44个素数 p（不大于257的素数共有55个）所对应的 M_p 都是合数。但是以后发现 M_{67} 和 M_{257} 不是

素数，而M_{61}，M_{89}，M_{107}却是素数*．M_p为素数时称为默森尼数（Mersenne's numbers）．据猜测有无穷多个默森尼数。

至今（1985年9月止）已有29个默森尼数，它们是

$p=2$，3，5，7，13，17，19，31，61，89，107，127，521，607，1279，2203，2281，3217，4253，4423，9689，9941，11213，19937（1971年3月由Turkerman给出M_{19937}是6002位的素数），21701（1978年10月Mr.Curb London Noll及Miss.Laura Nickel给出的M_{21701}是6533位素数），23209（1979年2月中学生诺尔在电子计算机上发现M_{23209}是一个6987位的素数），44497（1979年4月由计算机系统分析专家D．Slowinski和H．Nelson用高速电子计算机CRAT—Ⅰ型算出的13395位的素数），86243（1983年1月D．Slowinski给出M_{86243}是25692位的素数．他还验证了$44497<p\leqslant 62000$和$75000\leqslant p<86243$中无默森尼数，还差$62000<p<75000$未验证，从而猜测M_{86243}是第28个默森尼数．）1985年9月美国切夫隆公司副总经理威廉·巴茨在测试一部超级计算机时发现M_{216091}是一65050位的素数（它可能是第29或第30个默森尼数），这29个M_p都是素数．并且知道$p\leqslant 257$的其他43个素数p，M_p都是合数，如果$257<p<44497$的其他素数p（除$p=521$，…，44497等15个默森尼数之外），M_p都是合数，则斯洛温斯基（Slowinski）的猜测是有意义的。

* 欧拉在1732年阐明M_{41}和M_{47}是素数，但这是错误的．故最先发现默森尼错误的是，1886年波留森（Perrusin）和时洛霍夫（Seelhoff）发现M_{61}是素数。1903年柯里（Cole）证明

$$M_{67}=193707721\times 761838257287$$

并且这两个因数都是素数。

从定理1·16知道要a^n+1为奇素数时，必$n=2^m$，$a\geqslant 2$为偶数，因而费马（Fermat1601—1665）猜测：形如

$$F_n=2^{2^n}+1$$

的数都是素数．我们把F_n称为费马数．

最前面的五个费马数$F_0=3$，$F_1=5$，$F_2=17$，$F_3=257$，$F_4=65537$都是素数．

但是欧拉证明了$n=5$时，$F_5=2^{2^5}+1$就是合数．其证法如下：

$\because\quad F_5=2^4\cdot(2^7)^4+1,$

令$a=2^7$，$b=5\Longrightarrow a-b^3=3$，$1+ab-b^4=1+3b=2^4$，

$\therefore\quad F_5=(1+ab-b^4)a^4+1=(1+ab)a^4+(1-a^4b^4)$

$=(1+ab)[a^4+(1-ab)(1+a^2b^2)]=641\times 6700417$

是合数．

1880年林都利（Landry）证明了

$$F_6=2^{2^6}+1=274177\times 67280421310721.$$

至今已证明，$n=5$，6，7，8，9，10，11，12，13，14，15，16，17，18，19，21，23，25，26，27，32，36，38，39，42，55，58，63，73，77，81，117，125，144，150，207，226，228，250，267，268，284，316，452，1945时，F_n都是合数．其证明方法通用的有如下两种：

（1） Lucas定理：F_n的每一个因子都是形如$2^{n+2}k+1$的数．即F_n的因子都是下列算术级数的某些项：

$1,\ 2^{n+2}+1,\ 2\cdot2^{n+2}+1,\ 3\cdot2^{n+2}+1,\ \cdots.$

（2） Pepin检验法：F_n是素数的充要条件是F_n整除$3^{2^{(2^n-1)}}+1$．

用这个方法来检验F_n为合数是十分卓越的。由于证明了$F_{1945} + 3^{2^{(2^{1945}-1)}}+1$而　定$F_{1945}$是合数，1957年R·M·Robinson发现$5\cdot 2^{1947}+1 | F_{1945}$。这些都是惊人的成就，因为$F_{1945}$是一个580多位数。

1905年J·C·Morehead用Pepin法证明了F_7是合数，同年A·E·Western也独立证明了同一结果，直到1971年才由John Brillhart和Michael Morrison利用加利福尼亚大学洛杉矶分校的一台计算机才算出：

$$
\begin{aligned}
F_7 &= 2^{2^7}+1 = 2^{128}+1 \\
&= 340282366920938463374607431768211457 \\
&= 59649589127497217 \times 5704689200685129054721 .
\end{aligned}
$$

1909年Morehead和Western合作证明了F_8是合数。1980年初澳大利亚的Brent教授采用巧妙的算法，求得了F_8的最小素因数是1238926361552897，另一个因数是62位数。

由于上面的成果，因此有人提出反猜测：只有有限个数的费马数是素数。这对费马来说是很不幸的。

高斯曾证明，若F_n是素数，则正的F_n边形可以用规尺作图来画出，所以说费马数为素数的问题在几何上有它的特殊意义。

定理1·18　（算术基本定理）任一整数$a>1$，都可以表成有限个素数的连乘积，即

$$a = p_1 p_2 \cdots p_n, \tag{40}$$

其中 $p_1 \leqslant p_2 \leqslant \cdots \leqslant p_n$ 为素数。并且这种表示法是唯一的。

这个定理亦称唯一分解定理。

证明 用数学归纳法证明 a 分解式的存在性。

$a=2$时，(40)显然成立。

B，设对于一切小于 a 的正整数(40)都成立.为a时，若 a 是素数，则(40)式对 a 成立；若 a 是合数时，则有两个整数 b和C，满足条件

$$a=bc,\quad 1<b<a,\quad 1<c<a.$$

由归纳法假设

$$a=bc=p_1'\cdots p_e'\ p_{e+1}'\cdots p_n',$$

经过按$p_1'p_2'\cdots P_n'$的大小顺序排列后，得

$$a=p_1p_2\cdots p_n,\quad p_1\leqslant p_2\leqslant\cdots\leqslant p_n.$$

所以(40)对于任何自然数 a 都成立。

今证明这样的分解式是唯一的，若

$a=q_1q_2\cdots q_m$，$q_1\leqslant q_2\leqslant\cdots\leqslant q_m$为素数、则

$$q_1q_2\cdots q_m=p_1p_2\cdots p_n.$$

$$\therefore\quad q_1\,|\,p_1p_2\cdots p_n,\quad p_1\,|\,q_1q_2\cdots q_m\Longrightarrow q_1\,|\,p_i,p_1\,|\,q_j\Longrightarrow$$

$$\Longrightarrow q_1=p_i,p_1=q_j\text{且}p_i\geqslant p_1,q_j\geqslant q_1\Longrightarrow$$

$$\Longrightarrow q_1=p_i\geqslant p_1=q_j\geqslant q_1\Longrightarrow q_1=p_1.$$

同法可得$q_2=p_2$，$q_3=p_3$，…余此类推，可得 $m=n$ $q_m=p_n$。故分解式是唯一的。

唯一性的证明，也可以对 n 使用数学归纳法。

系 1 任一正整数 a 可以唯一地写成

$$a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$$

$$(p_1<p_2<\cdots<p_k,\alpha_i\geqslant 0,i=1,\cdots,k).\qquad(41)$$

系 2 若正整数 a 可分解成(41)式的形式，则 a 的任一正因数都可表成

$$d=p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta_k}\ (\alpha_i\geqslant\beta_i\geqslant 0,\ i=1,\ 2,\cdots,k)。\quad (42)$$

(41)式称为a的标准分解式(decomposition into standard form)，为了方便在(42)中引入了0次幂。

系 3 设a,b是任意两个正整数，且

$$a=p_1^{\alpha_1}\cdots p_k^{\alpha_k},\ b=p_1^{\beta_1}\cdots p_k^{\beta_k}(\alpha_i\geqslant 0,\beta_i\geqslant 0;\ i=1,\cdots,k)$$

则

$$(a,b)=p_1^{\gamma_1}\cdots p_k^{\gamma_k}\ (\gamma_i=\min(\alpha_i,\beta_i);\ i=b,\cdots,k);$$

$$[a,b]=p_1^{\delta_1}\cdots p_k^{\delta_k}\ (\delta_i=\max(\alpha_i,\beta_i);\ i=1,\cdots,k)。$$

其中$\min(\alpha_i,\beta_i)$和$\max(\alpha_i,\beta_i)$分别表示α_i,β_i中小的和大的一个。

系 3 的结论可以推广到多个正整数的情况。例如，求2400，360，141750的最大公因数和最小公倍数。

解：∵ $2400=2^5\times 3\times 5^2$;

$360=2^3\times 3^2\times 5$;

$141750=2\times 3^4\times 5^3\times 7$。

∴ $(2400,360,141750)=2\times 3\times 5=30$;

$[2400,360,141750]=2^5\times 3^4\times 5^3\times 7=2268000$。

结束本章之前再举几个例子。

例 1·11 定义在自然集到整数集里的函数f(x)，它满足

(1) $f(2)=2$;

(2) $f(m\cdot n)=f(m)\cdot f(n)$;

(3) 当$m>n$时，$f(m)>f(n)$。

证明：$f(n)=n$。

证明 由性质(1)和(2)知，

$$2=f(2)=f(1\cdot2)=f(1)\cdot f(2)=f(1)\cdot2,$$

$$\therefore\quad f(1)=1,$$

而且 $f(2^2)=f(2)\cdot f(2)=2\times2=2^2,\cdots,f(2^k)=2^k$ $(k=1,2,\cdots)$。

设 $n=2^k+h\ (k=1,2,\cdots;\ h=1,2,\cdots,2^k-1)$。这样的n就包含除1和$2^k$之外的一切正整数了。

$\because\quad 2^k<2^k+1<\cdots<2^k+2^k-1=2^{k+1}-1<2^{k+1}$，

由性质(3)及$f(2^k)=2^k$，有

$$2^k<f(2^k+1)<\cdots<f(2^{k+1}-1)<2^{k+1}$$

这表明了$f(2^k+h)$，$h=1,2,\cdots,2^k-1$ 是2^k与2^{k+1}之间2^k-1个不同的整数，而2^k和2^{k+1}之间刚好有2^k-1个整数，所以$f(2^k+h)=2^k+h$，即对一切自然数n都有$f(n)=n$。

若把此例的(1)改为$f(p)=p$，p为素数，该结论是否成立？若成立为什么？这留给读者作练习。

例1·12 设n是五位数（它的万位数字不是0），m是n中划掉它的中间某一位数字后所组成的四位数，试确定一切n，使得$\frac{n}{m}$是整数（即求出一切使$\frac{n}{m}=k$的整数n）。

解 设 $n=\overline{xyzuv}=x\cdot10^4+y\cdot10^3+z\cdot10^2+u\cdot10+v$，其中$x,y,z,u,v$都是$0,1,\cdots,9$中的一个数码，且$x\neq0$。$m=\overline{xyuv}=x\cdot10^3+y\cdot10^2+u\cdot10+v$，并且$k=\frac{n}{m}$是整数。

容易证明

$$9m<n<11m\Longrightarrow9<k<11.$$

事实上，

$$n-9m=(10-9)x\cdot10^3+(10-9)y\cdot10^2+z\cdot10^2$$
$$+(1-9)u\cdot10+(1-9)v$$

$$=10^3x+10^2y+10^2z-80u-8v>0;$$

$$11m-n=(11-10)x\cdot10^3+(11-10)y\cdot10^2-z\cdot10^2+(11-1)u\cdot10+(11-1)v$$

$$=10^3x+10^2y-10^2z+10^2u+10v>0.$$

因为 k 是整数，所以 $k=10$，于是 $n=10m$，即

$$x\cdot10^4+y\cdot10^3+z\cdot10^2+u\cdot10+v=x\cdot10^4+y\cdot10^3$$

$+u\cdot10^2+v\cdot10$，所以 x,y 可以是 $0,1,\cdots,9$ 中任意一个数码，且 $x\neq0$，而 z,u,v 满足下列方程组：

$$\begin{cases}z-u=0,\\u-v=0,\\v=0.\end{cases}$$

$$\therefore\ z=u=v=0,$$

于是 $n=\overline{xy000}=N\cdot10^3$，$10\leqslant N\leqslant99$。

例1·13 已知四个不同的整数 a,b,c,d 使得整系数多项式

$$f(x)=x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n\ (n\geqslant4)$$

的值有

$$f(a)=f(b)=f(c)=f(d)=5.$$

证明不存在整数 k，使得 $f(k)=8$。

证明 $f(x)-5$ 有四个根 a,b,c,d，所以

$$f(x)-5=(x-a)(x-b)(x-c)(x-d)g(x),$$

其中 $g(x)=x^m+b_1x^{m-1}+\cdots+b_m(m=n-4)$，且 $b_1,b_2,\cdots,b_m$ 都是整数。

如果存在整数 k，使得 $f(k)=8$，那末

$$(k-a)(k-b)(k-c)(k-d)g(k)=3.$$

而 3 是素数，它有且只有 ±1，±3 四个因数，于是上式的 $k-a,k-b,k-c$，$k-d$ 中至少有三个等于 1 或 -1，所以其

中有两个相等，这是矛盾的。

上述三例都选自加拿大、美国中学生数学竞赛的试题。按例1·13的思想方法，读者可编制若干类似的题目，如，

(i) 若把“5”改为“s”，“8”改为一个素数p和s之和“p+s”，其他条件不变，可得到同一性质的题目。

(ii) 已知五个不同的整数a,b,c,d,e使得整系数多项式

$$f(x)=x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n\ (n\geqslant 5)$$

的值有$f(a)=f(b)=f(c)=f(d)=f(e)=5$，证明不存在整数k，使得$f(k)=11$。

同样地，读者亦可把“5”改为“s”，“11”改为“$s+p_1p_2$”其中p_1,p_2是二素数。

例1·14 （上海市1956年竞赛题）

a. 设n是整数，证明$13^{2n}-1$是168的倍数；

b. 问具有哪些性质的自然数n能使$1+2+\cdots+n$整除$n!$？

解 a. $13^{2n}-1=(13^2)^n-1=(13^2-1)(13^{2(n-1)}$

$$+13^{2(n-2)}+\cdots+13^2+1)=168k(k\text{是整数})。$$

∴ $168|(13^{2n}-1)$。

b. $\because 1+2+\cdots+n=\dfrac{n(n+1)}{2}$，要讨论$\dfrac{n(n+1)}{2}\Big|\, n!$，只要讨论$(n+1)|\,2(n-1)!$ 的情况

(i) 当$n=2m+1$为正奇数时$\Longrightarrow n+1=2(m+1)$，$2(n-1)!=2\times(2m)!$

显然当$m=0$时，$2\times1\,|\,2\times0!$，当$m\geqslant1$时，$m+1\leqslant 2m\Longrightarrow 2(m+1)|2\times(2m)!\Longrightarrow n+1\,|\,2\cdot(n-1)!$

(ii) 当n是正偶数时，如果n+1是素数，那末$(n+1)\nmid 2\times(n-1)!$，因为$2\times(n-1)!$中任一因数都不是$p=n+1$的倍数。

如果n+1是合数，那末$n+1=ab, 3\leqslant a<\frac{n+1}{2}$，$3\leqslant b<\frac{n+1}{2}$，又因为n+1为奇合数，则n最小是8，所以$\frac{n+1}{2}<n-1$，更准确些$\frac{2(n+1)}{3}<n-1\ (n\geqslant 8)$。

当$a\neq b$时，a和b都是$(n-1)!$中的一个因数，故$(n+1)\mid 2\times(n-1)!$；

当$a=b$时$\Longrightarrow n+1=a^2\Longrightarrow a=\frac{n+1}{a}\ (a\geqslant 3)\Longrightarrow$
$\Longrightarrow 2a=\frac{2(n+1)}{a}\leqslant\frac{2(n+1)}{3}<n-1\ (n\geqslant 8)$。所以在$(n-1)!$中出现a和2a的因子，即$a^2\mid 2\times(n-1)!$。

总之，除n+1为奇素数的正整数n外，一切正整数n都有

$$(1+2+\cdots+n)\mid n!$$

例1·15 n是非负整数时，证明$73\mid 8^{n+2}+9^{2n+1}$

证明 $8^{n+2}+9^{2n+1}=64\times 8^n+9\times 81^n=73\times 8^n+9(81^n-8^n)=73[8^n+9(81^{n-1}+81^{n-2}\times 8+\cdots+8^{n-1})]$。

$\therefore\quad 73\mid 8^{n+2}+9^{2n+1}$。

例 1·16 当n是自然数时，证明$84\mid 4^{2n}-3^{2n}-7$。

证明 当$n=1$时，显然$84\mid 0$；设$n>1$，则

$$4^{2n}-3^{2n}-7=(16-9)(16^{n-1}+16^{n-2}\times 9+\cdots+9^{n-1})-7$$
$$=84t+7(4^{2n-2}+3^{2n-2}-1)$$

$$=84t+7(4\cdot 4^{2n-3}+3\cdot 3^{2n-3}-1)$$

$$=84t+7[4(4^{2n-3}-1)+3(3^{2n-3}+1)]$$

$$=84k.$$

此题亦可用数学归纳证明之。

例 1·17 (i) 对于任意自然数 n，证明，存在一个位数不超过 n 且各位数字都是 0 或 1 的自然数N，使得$n|N$。

(ii) 证明，存在一个位数不超过 1979（或1983）且各位数字都是 1 的自然数N，使得$1979|N$（$1983|N$）。

证明 (i) 因为$n+1$个数

$$0,1,11,111,\cdots,\overbrace{11\cdots\cdots1}^{n\text{位}}$$

中必有两个数a和b被n除后的余数相等，可设$a>b$，且

$$a=kn+r, b=hn+r \Longrightarrow N=a-b=(k-h)n \Longrightarrow n|N,$$

若a是s个 1 构成的s位数，b是t个 1 构成的t位数，则

$$N=a-b=\underbrace{1\cdots1}_{s-t\text{位}}\ \underbrace{0\cdots0}_{t\text{位}} \qquad (\alpha)$$

(ii) 同(i)的方法，知道取$n=1979$（1983）时，$1979|N$（$1983|N$，N是形如(α)右边的数），而1979（1983）与末位数字不等于 0 的数的积的末位数字是不等于 0，故

$$1979|\underbrace{11\cdots1}_{s-t\text{位}} \quad (1983|\underbrace{11\cdots1}_{s-t\text{位}}).$$

此例之(ii)是1979年全国数学竞赛的试题，它与例1·13都用到了"抽屉原则"，"抽屉原则"可作为生活常识来理解。

例 1·18 （上海57年竞赛题）写出十个连续的自然数，

个个都是合数。

解 如果一个数被2，3，…，11所整除，则把它加上 2，3，…，11所得的10个连续的自然数，就都是合数了（自然这十个连续数，可以是多种多样的，如，m，$m+1$，…，$m+9$，$m=k\times 11!+2$，k是任意自然数。），即

$$11!+2,\ 11!+3,\ \cdots,\ 11!+11;$$

或者

$$n!+2,\ n!+3,\ \cdots,\ n!+11\ (n\geqslant 11)$$

等等。

例 1·19 **一个六位数，当它分别乘以2，3，4，5，6时，所得的五个乘积仍然是六位数，而且每个六位数的全部数字都是原来六位数的数字，试求原来的六位数。**

解 显然原数的首位数字是1，否则它的五倍和六倍将是七位数。其次，首位数字是1的六位数的2，3，4，5，6倍所得的五个乘积的首位必是2，3，…，9中五个不同的数字，所以这个六位数，各位的数字都不相同，且不为0。

今再考虑末位数字，由于2，4，6，8的五倍及5的6倍的末位数字是0，故末位只可能是3，7，9之一，并要求它的2，…，6 倍的末位数字都不相同，并且含有1。

3 的2,3,4,5,6倍的末位数字是：6,9,2,5,8；

7 的2,3,4,5,6倍的末位数字是：4,1,8,5,2；

9 的2,3,4,5,6倍的末位数字是：8,7,6,5,4。

除7之外不包含1，故末位数字是7。中间四位数字必为4，8，5，2的一个排列。

下面研究第五位数字，它只能是2，4，5，8之一，而末两位数的2，3，4，5，6倍是：

$27\times 4=108$，出现0不是原数的数字，故第五位不能是

2．同理

47×2＝94，出现9故第五位不能是4．

57的1，2，3，4，5，6倍的倒第二位数字是5，1，7，2，8，4，刚好是原数的六个数字，所以第五位是5．实际上，87×3＝261，6不是原数的数字．

再从2，4，8中选取第四位数字．

257×3＝771，不对，457×2＝914出现9亦不对，所以第四位数字是8．

剩下第二、三位应排2和4．

4857×2＝9714，不对，所以原数是142857．

检验之，它的2，3，4，5，6倍分别是：285714，428517，571428，714285，857142．

此解法实际也是一种筛法（sieve method）．

习　　题

1．设n为任何整数，证明

（i）$6|n(n+1)(2n+1)$；

（ii）$6|n(n-1)(2n-1)$；

（iii）$8|[(2m+1)^2-1]$；

（iv）$6|n(n+1)(n+2)$．

2．证明一个整数能被2整除的充要条件是：它的个位数字是2的倍数．能被5整除的充要条件是：它的个位数字是0或5．能被3或9整除的充要条件是：它的各位数字之和是3或9的倍数．

3．证明，任意四个连续正整数之积加一，都是一个整数的平方．

4．当a是奇数时，$a(a^2-1)$是24的倍数．

5．证明，一个整数a，若不能被2和3所整除，则a^2+23是24的倍数．

6. 证明，$(3+\sqrt{5})^n+(3-\sqrt{5})^n$（n为任意自然数），是$2^n$的倍数。

7. 设 n 为正奇数时，$8|5^n+2\times 3^{n-1}+1$。

8. n是非负整数时，证明

（i） $19|5^{2n+1}\cdot 2^{n+2}+3^{n+2}\cdot 2^{2n+1}$；

（ii） $39|2^{6n+9}-5^{2n+1}$；

(iii) $49|2^{3n+3}-7n+41$。

9. n是任意整数时，证明

(i) $30|n^5-n$； (ii) $360|n^2(n^2-1)(n^2-4)$；

(iii) $6|n^3+11n$。

10. n是自然数时，证明

(i) $(n-1)^2|n^{n-1}-1$； (ii) $9|n^3+(n+1)^3+(n-1)^3$。

11. 用分解素因子的方法求最大公因数和最小公倍数。

(i) 48，84，120； (ii) 360，810，1260，3150。

12. 用辗转相除法求，51245，13310的最大公因数和最小公倍数。

13. 甲、乙、丙三班的学生数分别是54人、48人、72人，现要在各班中分别组织体育锻炼小组，但各小组的人数要相同，问锻炼小组的人数最多是多少人？这时甲、乙、丙三班各有几个小组？

14. 甲、乙、丙、丁四个齿轮互相啮合，齿数分别为84、36、60和48，问在转动过程中第一次同时啮合的各齿，到第二次再同时啮合时，各齿轮分别转过多少圈？

15. 证明，当且仅当$\frac{m}{a_1}$，$\frac{m}{a_2}$，…，$\frac{m}{a_n}$互素时，正整数m是诸正整数a_1，a_2，…，a_n的最小公倍数。

16. 我们用$\tau(m)$表示正整数m的正因数的个数，证明，当$m=p_1^{\alpha_1}\cdots p_n^{\alpha_n}$时，$\tau(m)=(\alpha_1+1)\cdots(\alpha_n+1)$，并计算$\tau(96)$，$\tau(168)$，$\tau(255)$，$\tau(121)$。

17. 我们用$S(m)$表示正整数m的一切正因数之和，证明，

当$m=p_1^{\alpha_1}\cdots p_n^{\alpha_n}$时，

$$S(m)=\frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdots\frac{p_n^{\alpha_n+1}-1}{p_n-1}.$$

18. 当n通过一切正整数时，形如$4n-1$的数中有无限多个素数。

19. 形如$6n+5$的素数数目是无限的。

20. 任何两个费马数都互素。

21. 将数$e=2.71828182845904\cdots$分解成简单连分数，求此连分数的前五个渐近分数。

22. 用连分数计算方程$x^2+9x+6=0$的两根，使它们准确到0.0001。

23. 用连分数计算方程$x^3-x^2-2x+1=0$的三个实根，使它准确到0.0001。

24. 计算欧拉括号

(i) $\{1, 0, 2, 0, 3\}$； (ii) $\{1, \frac{1}{2}, \frac{1}{2}, 2\}$；

(iii) $\{2, -2, 3, -3, 1, -4\}$； (iv) $\{\alpha, \beta, \gamma, \delta\}$；

(v) $\{3, 0, \frac{1}{2}, 0, 0, 1\}$.

25. 以$\{1, 2, 1, 3, 2, 3, 2\}$为例，当$m=3$时，来检验公式(30)。

26. 应用定理1·9的证明过程，求出以下列连分数为根的二次方程。

(i) $[\dot{2}, 4, 1, \dot{3}]$； (ii) $[\dot{1}, 2, 4, \dot{6}]$；

(iii) $[2,1,2,\dot{1},1,\dot{3}]$； (iv) $[4, \dot{1}, 1, 2, 1, 1, \dot{8}]$.

27. 用例1·10的方法，把61和137表成二自然数的平方和。

28. 若ax_0+by_0是形如$ax+by$（x，y是任意整数，a和b是两个不全为0的整数）的数中最小的正数，则

$$ax_0+by_0 \mid ax+by.$$

29. 若 a, b 是任意二整数，且$b\neq 0$，证明存在两个整数 s, t, 使得

$$a=bs+t,\quad |t|\leqslant\frac{|b|}{2}$$

成立，并且当 b 是奇数时，s, t 是唯一的，当 b 是偶数时，结果如何？

30. 证明整系数多项式

$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n$ $(n>0,\ a_0>0)$的x取任何整数时，有无限多个合数值.

31. 证明，当且仅当 $n=2^k-1$ 时，二项式 $(a+b)^n$ 的展开式的各项系数都是奇数。

32. (i) 求30! 的标准分解式；

(ii) 求250! 的标准分解式中3, 7, 11, 23诸素数的指数。

33. 设n为任意正整数，α, β是实数，证明：

(i) $[\alpha]+[\alpha+\frac{1}{n}]+\cdots+[\alpha+\frac{n-1}{n}]=[n\alpha]$;

(ii) $[2\alpha]+[2\beta]\geqslant[\alpha]+[\alpha+\beta]+[\beta]$;

(iii) $[\alpha]-[\beta]=[\alpha-\beta]$或$[\alpha-\beta]+1$.

34. (i) 设函数 f(x)在闭区间 $Q\leqslant X\leqslant R$ 上是连续的，并且非负，证明和式

$$\sum_{Q<X\leqslant R}[f(x)]$$

表示平面区域 $Q<X\leqslant R$, $0<y\leqslant f(x)$ 内的整点（整数坐标的点）的个数。

(ii) 设 p, q 是互素的奇正整数，证明：

$$\sum_{0<x<\frac{q}{2}}\left[\frac{p}{q}x\right]+\sum_{0<y<\frac{p}{2}}\left[\frac{q}{p}y\right]=\frac{p-1}{2}\cdot\frac{q-1}{2}.$$

(iii) 设 $r>0$, T是区域 $x^2+y^2\leqslant r^2$内的整点数，证明：

$$T=1+4[r]+8\sum_{0<x\leqslant\frac{r}{\sqrt{2}}}[\sqrt{r^2-x^2}]-4\left[\frac{r}{\sqrt{2}}\right]^2.$$

(iv) 设 $n>0$，T是区域 $x>0$，$y>0$，$xy\leqslant n$ 内的整点数，证明

$$T=2\sum_{0<x\leqslant\sqrt{n}}\left[\frac{n}{x}\right]-[\sqrt{n}]^2.$$

35. 设 n 是任一正整数，p 是素数，且

$$n=a_0+a_1p+a_2p^2+\cdots,\quad 0\leqslant a_i<p,$$

证明：在n! 的标准分解式中，素因数 p 的指数是

$$h=\frac{n-S_n}{p-1},$$

其中$S_n=a_0+a_1+a_2+\cdots$。

附录Ⅰ 哥德巴赫猜想

1742年6月7日普鲁士(今属德国)派往俄罗斯的一位公使哥德巴赫(Christain Goldbach)写信给欧拉，提出一个命题说："任何偶数，由4开始，都可以化成两个素数和的形式，任何奇数，由7开始都可以化成三个素数的和。"这是历史上著名的哥德巴赫猜想。猜想的第二部分实际是第一部分的推论，因为大于或等于7的奇数，都可以写成3(或奇素数p)加上一个大于或等于4的偶数之和，所以这个问题的第一部分若能解决，这个问题就全部解决了。因此通常说哥德巴赫猜想，就是指问题的第一部分。也就是："任何一个大于2的偶数，都是两个素数之和(表为1+1)"。欧拉表示，他相信哥德巴赫是对的，但他不能加以证明，而作为历史遗留的问题而提出，让后代的数学家共同努力，来判断该问题的是非。

1900年德国数学家希尔伯特(D·Hilbert)，在国际数学会的演说中，把哥德巴赫猜想看成是以往遗留的最重要的问题之一，介绍给20世纪的数学家来解决，即所谓希尔伯特第八问题的一部分。1912年德国数学家朗道在国际数学会的演说中，提出即使要证明较弱的命题：存在一个a，使每一个大于1的整数，都可以表成不超过a个素数之和(注意：猜想如果成立，即取a=3。)也是现代数学家所力不能及的！1921年英国数学家哈代在哥本哈根召开的数学会上说过，猜想的困难程度可以和任何没有解决的数学问题相比的。

近七十年来，哥德巴赫猜想吸引了世界上许多著名数学家的兴趣，并在证明上取得了很好的成绩。此外，研究这一猜想的方法，不仅对数论有广泛的应用，而且它可以用到不

少数学分支中去，推动了这些数学分支的发展。

下面简单介绍一些关于哥德巴赫猜想（下简称猜想）的主要成果。

早在1922年，英国数学家哈代和李特伍德（Hardy and Littlewood）提出一个研究猜想的方法，即所谓“圆法”，1937年苏联数学家依·维诺格拉朵夫（И·М·Виноградов）应用圆法，结合他创造的三角和估计方法证明了每一个充分大的奇数都是三个素数之和，从而基本上证明了猜想的第二部分，这就只差（1＋1）是正确的还没有证明了（因为第二部分并不包含第一部分，而第一部分却包含有第二部分）。

1920年，挪威数学家布朗改进了有两千多年历史的爱拉多染尼（Eratosthenes）氏“筛法”*，证明了每个充分大的偶数，都是两个素因子个数不超过9的正整数之和，我们把布朗的结果记为（9＋9）。1930年苏联数学家史尼尔曼用他创造的整数“密率”结合布朗筛法证明了朗道在1912年提出的问题，即证明“除1以外的任何正整数都可以化成不超过k（或a）个素数之和的形式，其中k是一个固定的数”。开始常数k是一个很大的数，后来下降到k＝69，但其方法不及三角和方法精密，德国数学家拉代马哈在1924年证明了（7＋7），英国数学家埃里特曼于1932年证明了（6＋6），苏联数学家布赫文塔布于1938与1940年分别证明了（5＋5）和（4＋4），这和运动员一样，不断刷新世界纪录。

我国数学家华罗庚早在30年代研究猜想，得到很好的成

---

* 爱氏筛法，是用$p\leqslant\sqrt{n}$的一切素数p来试除n，若这些p都不整除n，则n是素数，这样依次检验n＝2，3，4，…，是否素数，从而逐步在自然数列中筛出素数。

果，他证明了对于“几乎所有”的偶数，猜想都是对的，解放不久他就倡议并指导他的一些学生研究猜想，取得了很多成果，就获得国内外高度的评价，1956年我国数学家王元证明了（3+4），同一年苏联数学家维诺格拉朵夫又证明了（3+3），1957年王元证明了（2+3），这些结果的缺点是两个相加数中，还没有一个肯定为素数的。

早在1948年，匈牙利数学家瑞尼就证明了（1+b），这里的b是一个常数，用他的方法定出的b将是很大的，所以并没有人具体定出b的值。直到1962年我国数学家潘承洞与苏联数学家巴尔巴恩各自独立证明了(1+5)1963年潘承洞、巴尔巴恩、王元又证明了（1+4），1965年维诺格拉朵夫、布赫塔布与意大利数学家朋比巴证明了（1+3），我国数学家陈景润在对筛法作了新的重要改进之后，终于1966年证明了（1+2），取得迄今世界上关于猜想最好的成果。正因为陈氏定理的重要，目前世界上共有四个简化证明，最简单的是我国王元、丁夏畦、潘承洞的证明。

由上所述不难看出，哥德巴赫猜想，也象其他经典问题一样，它的一切成果，都是在前人成就的基础上，通过迂回曲折的道路而得到的。

附录Ⅱ 欧拉公式

这是一个用解析方法证明数论问题的例子，欧拉公式与他所证明的素数个数是无限的定理有密切的联系。

设 p_λ是任意素数，而$k>1$，则有

$$\frac{1}{1-\frac{1}{p_\lambda^k}}=1+\frac{1}{p_\lambda^k}+\frac{1}{p_\lambda^{2k}}+\frac{1}{p_\lambda^{3k}}+\cdots \qquad (1)$$

我们取不超过已知数N的所有素数，设它们是：$p_1=2$，$p_2=3$，$p_3=5$，…，p_n，我们就这些素数写出公式（1），并把这些公式的两边分别连乘，并按递减的顺序来排列乘积的各项。得

$$\prod_{\lambda=1}^{n}\frac{1}{1-\frac{1}{p_\lambda^k}}=1+\frac{1}{2^k}+\frac{1}{3^k}+\frac{1}{4^k}+\cdots+\frac{1}{N^k}+\frac{1}{N_1^k}+\frac{1}{N_2^k}+\cdots \qquad (2)$$

因为p_1，p_2，…，p_n是小于N的所有素数，显然等式(2)右边的前N项都已写出，其次，$N<N_1<N_2<\cdots$，一般情况$N_1\geqslant N+1$，$N_2\geqslant N_1+1$，…，即在N后面的自然数并非全部会在N_1，N_2，…中出现。可是当$k>1$时，级数$1+\frac{1}{2^k}+\frac{1}{3^k}+\cdots$是收敛的，因而对于任意小的$\varepsilon>0$，总可以找到自然数N，使得

$$\frac{1}{(N+1)^k}+\frac{1}{(N+2)^k}+\cdots<\varepsilon,$$

即，更加有$\frac{1}{N_1^k}+\frac{1}{N_2^k}+\cdots<\varepsilon$。因此，当$p_n$的下标n无限增加时，也就是N无限增大，这时我们从等式（1）知道无穷积$\prod_{\lambda=1}^{\infty}\frac{1}{1-\frac{1}{p_\lambda^k}}$是收敛的，并从而得到：欧拉公式

$$\prod_{\lambda=1}^{\infty}\frac{1}{1-\frac{1}{p_\lambda^k}}=\prod_{m=1}^{\infty}\frac{1}{m^k} \qquad (3)$$

（3）表示了任何自然数都可唯一地表成素数的乘积。而（2）当$k=1$时仍然成立，从而得到欧拉公式的推论。

$$\prod_{\lambda=1}^{n}\frac{1}{1-\frac{1}{p_\lambda}}>\sum_{m=1}^{N}\frac{1}{m} \qquad (4)$$

今设N无限增加，则n也无限增加，但是当$N\to\infty$时，（4）的右边是调和级数，故发散，因此（4）左边的无穷积亦发散。也就是

$$-\sum_{\lambda=1}^{\infty}\ln\left(1-\frac{1}{p_\lambda}\right).$$

发散，并且它的和$\to+\infty$。

但是当$\frac{1}{p}=\eta\leqslant\frac{1}{2}$时，$-\ln(1-\eta)=\eta+\frac{\eta^2}{2}+\frac{\eta^3}{3}+\cdots<\eta+\eta^2+\eta^3+\cdots=\frac{\eta}{1-\eta}<2\eta$。这就是说，级数

$2\sum_{\lambda=1}^{\infty}\frac{1}{p_\lambda}$，亦即级数$\sum_{\lambda=1}^{\infty}\frac{1}{p_\lambda}$是发散的。

因而有级数

$$\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\cdots=\sum\frac{1}{p} \quad (5)$$

是发散的，其中 p 过一切素数。

第二章　不 定 方 程

中国古代数学家张丘建，曾经解答了下面的题目：

"鸡翁一，值钱五，鸡母一，值钱三，鸡雏三，值钱一，百钱买百难，问鸡翁、母、雏各几何？"

设用x、y、z 分别代表鸡翁、鸡母、鸡雏的数目，就得到下面的方程：

$$5x+3y+\frac{1}{3}z=100,$$

$$x+y+z=100.$$

消去z，再化简得

$$7x+4y=100.$$

要解决这个问题，就是求出上述方程与方程组的非负整数解。该方程是一个二元一次不定方程的具体例子。一般地，一元二次不定方程，指的是，a，b，c 为整数的方程

$$ax+by=c.$$

本章主要介绍二元一次不定方程有整数解的条件及其解法，并推广于多元一次不定方程，最后介绍勾股数及费马大定理。

第一节　二元一次不定方程

本节将讨论二元一次不定方程有整数解的条件，并且说明在有解的情况下如何求出它的一切整数解。

假定给定二正整数 a和b(a>b)，用欧几里德除法求得a，b的最大公因数 d 由前章等式(32)知道，不定方程

$$ax+by=d \tag{1}$$

恒有整数解。

当$\frac{a}{b}=[q_1,q_2,\cdots,q_{n-1},q_n]$时，其解为

$$y_0=(-1)^{n-1}\{q_1,\cdots,q_{n-1}\},$$
$$x_0=(-1)^n\{q_2\cdots,q_{n-1}\} \qquad (2)$$

当$a>b>0$时，x_0,y_0有不同的符号。当$a>0$，$b<0$时，可以把(1)写作

$$ax+|b|(-y)=d。 \qquad (1)$$

当$\frac{a}{|b|}=[q_1,q_2,\cdots,q_n]$时，其解为

$$(-y_0)=(-1)^{n-1}\{q_1,\cdots,q_{n-1}\},\ x_0=(-1)^n\{q_2,\cdots,q_{n-1}\} \qquad (2)$$

若把(1)的两边同约去d，得

$$a_1x+b_1y=1 \qquad (1')$$

则(2)仍是它的一个整数解，其中$a=a_1d,b=b_1d$，$(a_1b_1)=1$。

因此(1)的求解问题，归结为

$$ax+by=1 \quad (a,b)=1 \qquad (3)$$

的求解问题。

下面研究一般的二元一次不定方程（uncertain equation）

$$ax+by=c \qquad (4)$$

其中a,b是非零整数，c是任意整数，我们有下面的基本定理：

定理2·1 不定方程(4)有解的充要条件是：$d|c$，其中$d=(a,b)$。

并且当(x_0,y_0)是它的一个解时，其一切解是：

$$\begin{cases} x_t = x_0 - \dfrac{b}{d}t, \\ y_t = y_0 + \dfrac{a}{d}t. \end{cases} \quad (t = 0, \pm 1, \pm 2, \cdots) \tag{5}$$

注意：这里及本章后面所指的“解”无特别声明，都指整数解。

证明 先证解的存在条件，若(4)有整数解(x_0, y_0)，则$ax_0 + by_0 = c$，因为$d|a, d|b$，所以$d | c$。

反之，若$d|a, d|b, d|c$，则$a = a_1d$，$b = b_1d$，$c = c_1d$，a_1, b_1, c_1都是整数，$(a_1, b_1) = 1$，(4)的两边同约掉d，得与(4)同解的不定方程

$$a_1x + b_1y = c_1, (a_1, b_1) = 1. \tag{4'}$$

由上面的分析知方程

$$a_1x + b_1y = 1 \tag{1'}$$

有解(2)。用(x_0', y_0')表示(1′)的一个解，令$x_0 = c_1x_0'$，$y_0 = c_1y_0'$，则(x_0, y_0)就是(4)的一个解。

其次，证明定理的后一部分，若(x, y)是(4)的任意解，则

$$ax_0 + by_0 = c \text{ 且 } ax + by = c,$$

$$\therefore \quad a(x - x_0) = -b(y - y_0). \tag{6}$$

两边同除以d，得

$$a_1(x - x_0) = -b_1(y - y_0), (a_1, b_1) = 1.$$

$$\therefore \left(-\frac{b}{d}\right) \Big| x - x_0, \quad \frac{a}{d} \Big| y - y_0 \Longrightarrow \begin{cases} x - x_0 = -\dfrac{b}{d}t, \\ y - y_0 = \dfrac{a}{d}t'. \end{cases}$$

$$\Longrightarrow\begin{cases} x = x_0 - \dfrac{b}{d}t, \\ y_0 = y_0 + \dfrac{a}{d}\,t'. \end{cases}$$

但要满足等式(6)，必须$t = t'$，事实上，由(6)得

$$\begin{cases} a(x_0 - \dfrac{b}{d}\,t - x_0\,) = -\dfrac{ab}{d}t \\ -b\,(y_0 + \dfrac{a}{d}t' - y_0) = -\dfrac{ab}{d}t' \end{cases} \Longrightarrow t = t'.$$

也就是说，(x,y)是(4)的解时，一定是(5)的形式。反之，(5)中t取任意整数时，都是(4)的解。事实上，

$$a\left(x_0 - \frac{b}{d}t\right) + b\left(y_0 + \frac{a}{d}\,t\right) = ax_0 + by_0 = c.$$

从定理2·1知道，(4)有解时，要求它的一切整数解，先求(1)的一个整数解(x_0', y_0')，次令$x_0 = \dfrac{c}{d}\,x_0'$，$y_0 = \dfrac{c}{d}\,y_0'$就得到(4)的一个整数解(x_0, y_0)，再用公式(5)给出(4)的一切整数解。

求x_0'，y_0'时，不管a,b是正或负，都取其绝对值，把符号合于x，y中，来求$|a|X + |b|\,Y = d$的解，其中$X = \pm x$，$Y = \pm y$，X与a同号，Y与b同号。当$|a| \geqslant |b|$ $(|b| > |a|)$时，把$|a|/|b|$ $(\,|b|/|a|)$化成连分数$[q_1, q_2, \cdots, q_n]$，则$Y_0 = (-1)^{n-1}\{q_1, \cdots, q_{n-1}\}$，$X_0 = (-1)^n \{q_2, \cdots, q_{n-1}\}$（或$X_0 = (-1)^{n-1}\{q_1, \cdots, q_{n-1}\}$，$Y_0 = = (-1)^n \cdot \{q_2, \cdots, q_{n-1}\}$），求得$x_0$，$y_0$后，仍用公式(5)求(4)的一般解。

例2·1 求方程

$$15x+19y=1$$

的整数解。

解 应用辗转相除法，求出q_i

$$19:15=1=q_1$$
$$15:4=3=q_2$$
$$4:3=1=q_3$$
$$3:1=3=q_4$$

$\therefore\ \frac{19}{15}=[1,\ 3,\ 1,\ 3]$。

本例因19>15，所以由公式(2)得

$x_0=(-1)^{4-1}\{1,\ 3,\ 1\}=-5$，$y_0=(-1)^4$

$\{3,\ 1\}=4$。一般解是

$x=-5\pm19t$，$y=4\mp15t\ (t=0,\ 1,\ 2,\ \cdots)$。

例2·2 求方程

$$126x-102y=18$$

的整数解

解 $(126,\ 102)=6$，$6|18$，故有解。方程两边同约去6，得

$$21x-17y=3。\tag{a}$$

先解方程

$$21x+17(-y)=1。$$

我们有$\frac{21}{17}=[1,\ 4,\ 4]$，$x_0'=-\{q_2\}=-4$，$-y_0'=\{q_1q_2\}=\{1,\ 4\}=5$，即$y_0'=-5$，故原方程(a)的解是：$x_0=-4\times3=-12$，$y_0=-5\times3=-15$。一般解是

$x_t=-12+17t$，$y_t=-15+21t\ (t=0,\ \pm1,\pm2,\cdots)$。

我国早在宋朝，数学家秦九韶的《数书九章》里，就用大衍求一术来求不定方程的整数解。在《数书九章》里记载有“余米推数”问题：某米店有相同容量的三箩米被盗，盗后左箩剩一合，中箩剩一升四合，右箩剩一合。破案后，知道甲、乙、丙三贼分别用一升九合，一升七合，一升二合的容器量盗左、中、右三箩，问共失米多少？三贼各盗去米多少？答案是：共失米九石五斗六升三合，甲、丙各盗三石一斗九升二合，乙盗米三石一斗七升九合。（这段话是白话译文）

此问题是解下列不定方程组

$$\begin{cases} x = 19y_1 + 1, \\ x = 17y_2 + 14, \\ x = 12y_3 + 1. \end{cases} \tag{7}$$

而实际上，是求(7)的最小正整数解。其解法是：

行次	定母 b_i	衍数 $=\frac{[b_1,b_2,b_3]}{b_i}$	衍母 $=[b_1,b_2,b_3]$	乘率	用数=衍数×乘率	剩数 C_i	各总=用数×剩数 x
1	19	204	[19,17,12] = 3876	15	3060	1	3060
2	17	228		5	1140	14	15960
3	12	323		11	3553	1	3553

“求1”主要是求“乘率”使它与衍数之积（用数），被定母除其余数为1．秦九韶的求法是：

$204\times1=19q_1+14(q_1=10)$,

$204\times2=19q_2+9(q_2=2q_1+1=21)$,

$204\times3=19q_3+4(q_3=q_1+q_2+1=32)$,

$204\times3\times5=19q_4+1(q_4=5q_3+1=161)$.

所以（7）的第一式的乘率是15，即 $x=204\times15=3060$，$y_1=161$是（7）第一式的一个正整数解，同理

$228\times1=17q_1+7(q_1=13)$，

$228\times2=17q_2+14(q_2=2q_1=26)$，

$228\times3=17q_3+4(q_3=q_1+q_2+1=40)$，

$228\times5=17q_4+1(q_4=q_2+q_3+1=67)$。

所以（7）的第二式的乘率是5，$x=228\times5=1140$，$y_2=67$是$x=17y_2+1$的整数解，两边同乘以14得，$x=1140\times14==15960$，$y_2=67\times14=938$是（7）第二式的一个正整数解。

$323\times1=12q_1+11(q_1=26)$，

$323\times11=12q_2+1(q_2=11q_1+10=296)$。

所以（7）的第三式的乘率是11，$x=3553$，$y_3=296$是（7）第三式的正整数解。

而此题的目的是求出不定方程组（7）共同的正整数解x，表中的各总，就是（7）的各式的正整数解，第一式的各总被17、12所整除而被19除余1；第二式的各总被19、12所整除而被17除余14；第三式的各总被19、17所整除而被12除余1，所以它们的和

$x=3060\times1+1140\times14+3553\times1=3060+15960+3553=22573$是满足方程组（7）的$x$值（这时$y_1=161+\frac{15960+3553}{19}$，同样可求$y_2$，$y_3$的变化后的值），但这里所求的$x$值，并不是$x$的最小正整数解。减去衍母〔19，17，12〕$=3876$的倍数后，仍是（7）的解，所以本问题的解答是$x=22573-5\times3876=3193$（合）。这就是说每箩储米三石一斗九升三合。

$3193-1=3192$（左箩被盗的谷数），

$3193-14=3179$（中箩被盗的谷数），

$3193-1=3192$（右箩被盗的谷数）。

此法亦适用于解一元一次同余式组，这将在第四章第二节中再说。

例2·3 用大衍术一术求不定方程

$$19x=15y+1 \tag{8}$$

的正整数解。

解 只有一个方程时，可把 x 的系数看作衍数，y 的系数看作定母。

$19\times 1=15q_1+4(q_1=1)$，

$19\times 2=15q_2+8(q_2=2)$，

$19\times 4=15q_3+1(q_3=2q_2+1=5)$。

所以（8）有正整数解 $x_0=4$，$y_0=5$，一般地

$x=4+15t$，$y=5+19t$（$t=0$，1，2，…）

都是（8）的正整数解。

第二节　多元一次不定方程

所谓多元一次不定方程，指的是整系数方程

$$a_1x_1+a_2x_2+\cdots+a_nx_n=b\ (n\geqslant 2), \tag{9}$$

不失掉讨论问题的一般性，可设 a_1，a_2，…，a_n 都不等于 0。今先证

定理2·2 （9）有整数解的充要条件是：$(a_1,\cdots,a_n)|b$。

证明 设 $(a_1, a_2\cdots, a_n)=d$，若（9）有整数解 $(x_1'$，x_2'，…，$x_n')$，则

$$a_1x_1'+a_2x_2'+\cdots+a_nx_n'=b$$

为整数的等式，而$d|a_1$，$d|a_2,\cdots$，$d|a_n$，由整除的性质3°知道，$d|b$。

反之，若$d|b$，我们用数学归纳法，证明(9)有整数解。

A）当$n=2$时，由定理2·1知(9)有整数解。

B）设为$n-1$时，(9)有整数解，今证明为n时(9)亦有整数解。

令$d_2=(a_1, a_2)$，$(d_2, a_3, \cdots, a_n)=d$，$d|b$，由归纳法假设知，方程

$$d_2t_2+a_3x_3+\cdots+a_nx_n=b$$

有整数解，设其一解为$(t_2', x_3', \cdots, x_n')$．再考虑

$$a_1x_1+a_2x_2=d_2t_2'.$$

由定理2·1及$(a_1, a_2)=d_2$知上式有整数解，设其一解为(x_1', x_2')，则

$$a_1x_1'+a_2x_2'+a_3x_3'+\cdots+a_nx_n'$$

$$=d_2t_2'+a_3x_3'+\cdots+a_nx_n'=b.$$

故$(x_1', x_2', \cdots, x_n')$是(9)的一个整数解。

定理2·2已提供了一个求(9)整数解的方法，即先求出$(a_1, a_2)=d_2$，$(d_2, a_3)=d_3$，$\cdots$，$(d_{n-1}, a_n)=d_n$，则$d_n=(a_1, \cdots, a_n)=d$，由定理2·2已知若$d_n|b$，则(9)有整数解，若$d_n\nmid b$，则(9)没有整数解．作方程

$$\begin{aligned}&a_1x_1+a_2x_2=d_2t_2,\\&d_2t_2+a_3x_3=d_3t_3,\\&\cdots\quad\cdots\quad\cdots,\end{aligned}\tag{10}$$

$$d_{n-2}t_{n-2}+a_{n-1}x_{n-1}=d_{n-1}t_{n-1},$$
$$d_{n-1}t_{n-1}+a_nx_n=b.$$

首先，按前节所给的方法求出最后一个方程的整数解；次把 t_{n-1} 代入倒数第二个方程后，再求出它的整数解；依此类推，可求出(9)的整数解。(10)的一组方程中 t_{n-1}，t_{n-2}，…，t_2 都可以看作是常数。

例2·4 求 $9x+24y-5z=1000$ 的一切整数解。

解 $(9, 24)=3$，$(3, -5)=1$ 故该方程有整数解。考虑方程

$$9x+24y=3t，即 3x+8y=t,$$

及 $$3t-5z=1000.$$

用第一节的方法，解得

$$\begin{cases}x=3t-8u,\\ y=-t+3u;\end{cases}\quad (u=0,\ \pm1,\ \pm2,\ \cdots)$$

$$\begin{cases}t=2000+5v,\\ z=1000+3v.\end{cases}\quad (v=0,\ \pm1,\ \pm2,\ \cdots)$$

消去 t，得

$$x=6000+15v-8u,$$
$$y=-2000-5v+3u,$$
$$z=1000+3v.\ (u,\ v=0,\ \pm1,\ \pm2,\ \cdots)$$

就是所要求的一切整数解。

第三节 勾股数

本节里所研究的一种特殊的二次不定方程，在我国古算书《周髀算经》中，已经载有："句广三，股多四，径偶五."（句是"勾"的古写），这是一个三边长都是整数的直角三角形。因此已经知道了不定方程

$$x^2+y^2=z^2 \tag{11}$$

有一组整数解（3，4，5）（后面仍用解代表整数解）。刘徽九章注（263年）中又载有$5^2+12^2=13^2$，$8^2+15^2=17^2$，$7^2+24^2=25^2$，$20^2+21^2=29^2$，由此可知，我国古代数学家已经给出了(11)的许多组解，本节的目的是给出(11)的一切解。

显然$x=0$，$y=0$，$z=0$；$x=0$，$y=\pm z$；$y=0$，$x=\pm z$都是(11)的解。除此之外，(11)的每一组解都不包含0。要求(11)的一切非零解（指的是x，y，z都不等于0的解），只要求出它的一切正整数解就可以了，因此可设$x>0$，$y>0$，$z>0$。

若(11)有非零解，且$(x,y)=d>1$，则$d^2|x^2+y^2$，即$d^2|z^2 \Longrightarrow d|z$，因此可把(11)的两端同约去$d^2$，也就是，只须求$(x,y)=1$的解。

引理1 若(11)有非零解，且$(x,y)=1$时，则它的任一非零解的x，y总是一奇一偶。

证明 因为$(x,y)=1$，所以x，y不能同为偶数，如果$x=2k+1$，$y=2h+1 \Longrightarrow x^2=4m+1$，$y^2=4n+1$，其中$m=k^2+k$，$n=h^2+h \Longrightarrow x^2+y^2=4(m+n)+2\neq z^2$。事实上，$z^2$只能是$4s$或$4s+1$形的数。所以x，y只能是一奇一偶。

由引理1，可设在（i）$x>0$，$y>0$，$z>0$；（ii）$(x,y)=1$；（iii）x是偶数，y是奇数等三条件下，求(11)的整数解。

引理2 不定方程

$$uv=w^2,\ w>0,\ u>0,\ v>0,\ (u,v)=1. \tag{12}$$

的一切正整数解，可以写成公式：

$$u=a^2, v=b^2, w=ab, a>0, b>0, (a,b)=1. \tag{13}$$

证明 设(u, v, w)是(12)的一个解，令

$u=a^2u_1$，$v=b^2v_1$，$a>0$，$b>0$，其中u_1，v_1不再被任何大于1的整数的平方所整除，则$a^2|w^2$，$b^2|w^2$，因此$a|w$ $b|w$，又因为$(u, v)=1$，故$(a, b)=1$，从而得到$ab|w$，故$w=w_1ab$，代入(12)得

$$a^2b^2u_1v_1=a^2b^2w_1^2 \Longrightarrow u_1v_1=w_1^2$$

上式的$w_1=1$，事实上，若$w_1\neq1$，则存在素数p使得

$p^2|w_1^2 \Longrightarrow p^2|u_1v_1$，这与$u_1$，$v_1$的定义及$(u_1, v_1)=1$的假设矛盾，所以$u_1=v_1=1$，且

$$u=a^2,\ v=b^2,\ w=ab,\ a>0,\ b>0,\ (a, b)=1。$$

反之，(13)式中的(u, v, w)显然是(12)的解。

定理2·3 不定方程(11)的适合条件

$$x>0,\ y>0,\ z>0,\ (x, y)=1,\ 2|x \tag{14}$$

的一切正整数解，可以用下列公式表示出来：

$$x=2ab,\ y=a^2-b^2,\ z=a^2+b^2 \tag{15}$$

其中$a>b>0$，$(a, b)=1$，a，b一奇一偶。

证明 (i)把(15)代入(11)得

$$x^2+y^2=(2ab)^2+(a^2-b^2)^2=(a^2+b^2)^2=z^2。$$

所以(15)是(11)的解，且$x>0$，$y>0$，$z>0$，$2|x$，$2\nmid y$，设$d=(x, y)$，则$d^2|z^2$，$d|z$，因此

$$d|a^2+b^2,\ d|a^2-b^2 \Longrightarrow a^2+b^2=kd,\ a^2-b^2=hd$$

$$\Longrightarrow 2a^2=(k+h)d,\ 2b^2=(k-h)d \Longrightarrow d|2(a^2, b^2)，但$$

$$(a, b)=1 \Longrightarrow d=1或2，又因\ y\ 是奇数 \Longrightarrow d=1.$$

即$(x, y)=1$，所以(15)是满足条件(14)的不定方程(11)的解。

(ii) 今证明(11)适合条件(14)的任一正整数解，都可

以写成(15)的形式。

设(x, y, z)是(11)的适合条件(14)的任一正整数解，则$2|x$，$(x, y)=1$，因此，y，z都是奇数，而

$$\left(\frac{x}{2}\right)^2=\frac{z+y}{2}\cdot\frac{z-y}{2}$$

其中$\left(\frac{z+y}{2}, \frac{z-y}{2}\right)=1$，否则，若$\left(\frac{z+y}{2}, \frac{z-y}{2}\right)=d>1$，则

$$z+y=2kd,\ z-y=2hd\Longrightarrow 2z=2(k+h)d,\ 2y=2(k-h)d\Longrightarrow d|z,\ d|y\Longrightarrow d|x$$

这与$(x, y)=1$矛盾，所以$d=1$。

于是由引理2知，有整数a，b存在，使得下式成立：

$$\frac{z+y}{2}=a^2,\ \frac{z-y}{2}=b^2,\ \frac{x}{2}=ab,\ a>0,\ b>0,$$

$$(a, b)=1\Longrightarrow x=2ab, y=a^2-b^2, z=a^2+b^2, (a,b)=1.$$

由$y>0$知$a>b$，又由y是奇数，知a，b一奇一偶。

把(11)改写为$\left(\frac{x}{z}\right)^2+\left(\frac{y}{z}\right)^2=1$，由定理2·3即得

系　单位圆上的一切有理点，可以表成

$$\left(\pm\frac{2ab}{a^2+b^2},\ \pm\frac{a^2-b^2}{a^2+b^2}\right)及\left(\pm\frac{a^2-b^2}{a^2+b^2}, \pm\frac{2ab}{a^2+b^2}\right),$$

其中a，b不全为0，正负号可以任意选取。

在系里可以看到单位圆上有无穷多个有理点，但是否可推广到：任一二次曲线上都有无穷多个有理点呢？不对！如，双曲线

$$X^2-3Y^2=2$$

上并无有理点。事实上，令$X=\frac{x}{z}$，$Y=\frac{y}{z}$，$(x,y,z)=1$，则其有理点是

$$x^2-3y^2=2z^2 \text{即} x^2-2z^2=3y^2, \ (x, \ y, \ z)=1$$

的整数解。由于$(3m+1)^2=3k+1$，$(3m+2)^2=3h+1$，所以上方程若有解，必$3|x$，$3|z \Longrightarrow 3|y$，这与$(x, y, z)=1$矛盾．一般地

定理2·4 在不是直线的有理系数的二次曲线上如有一有理点，则有无穷多个有理点．

证明 可设该曲线经过原点，即原点是它的一个有理点（否则，可以把坐标轴平行移动到$x'=x-x_0$，$y'=y-y_0$，(x_0, y_0)是该曲线上的一个有理点）．此二次曲线可以写成

$$S_2(x, \ y)+S_1(x, \ y)=0$$

其中$S_i(x, y)$是x，y的i次齐次式．若$S_1(x, y)$恒等于0，则原二次曲线蜕化为两条直线（椭圆型是一点，双曲型是二相交直线，抛物型是一条直线）；若$S_2(x, y)$恒等于0，则原二次曲线为一直线．所以$S_1(x, y)$和$S_2(x, y)$都不恒等于0．令$y=\lambda x$，则

$$xS_2(1, \ \lambda)+S_1(1, \ \lambda)=0$$

$$\therefore \quad x=-\frac{S_1(1, \ \lambda)}{S_2(1, \ \lambda)}, \quad y=-\frac{\lambda S_1(1, \ \lambda)}{S_2(1, \ \lambda)},$$

其中λ为任一有理数，故该二次曲线上有无穷多个有理点．

定理2·5 设A，B，C是不全为零的有理数，若B^2-4AC是一有理数的平方，则二次曲线

$$Ax^2+Bxy+Cy^2+Dx+Ey+F=0 \tag{a}$$

上有无穷多个有理点．

证明 设$B^2-4AC=L^2$，则

$$Ax^2+Bxy+Cy^2=A\left[\left(x+\frac{B}{2A}y\right)^2-\frac{L^2}{4A^2}y^2\right]$$

$$=A\left(x+\frac{B-L}{2A}y\right)\left(x+\frac{B+L}{2A}y\right).$$

(i) 若$L\neq0$，令

$$x'=x+\frac{B+L}{2A}y,\ y'=x+\frac{B-L}{2A}y$$

代入(a)式得

$$Ax'y'+D'x'+E'y'+F=0$$

其中$D'=\dfrac{DL-BD+2AE}{2L}$，$E'=\dfrac{DL+BD-2AE}{2L}$，解得

$$x'=-\frac{E'y'+F}{Ay'+D'} \tag{b}$$

满足(b)的有理数对(x', y')有无穷多对，故在(a)上的有理点有无穷多个。

(ii) 若$L=0$（抛物线型），令

$$x'=x+\frac{B}{2A}y,\ y'=-y,$$

代入(a)得

$$Ax'^2+D'x'+E'y'+F=0,$$

其中$D'=D$，$E'=\dfrac{BD-2AE}{2A}$若$E'\neq0$，则

$$y'=-\frac{1}{E'},\ (Ax'^2+Dx'+F) \tag{c}$$

(c)中取任一有理数x'得到有理数y'，对应于(a)上一个有理点(x, y)，所以(a)上有无穷多个有理点。

若$E'=0$，则(a)已非二次曲线。

由定理2·4，2·5可以推出：若

$$f(x_1, x_2, \cdots, x_n)=0 \tag{d}$$

是一个$x_1, x_2, \cdots, x_n$的整系数的二次齐次式（不能分解为一次式之积），则具备什么条件时，(d)上的整点个数是无穷的？

在定理2·4中，令$x=\frac{x'}{z'}$，$y=\frac{y'}{z'}$，就是一个三个未知数的二次齐次式，它的一切有理点就是该齐次式的非原点的整点。所以当 $n\geqslant3$时，(d)若有一非原点的整点，则它有无穷多个整点。但是何时(d)上有一非原点的整点呢？例如，

$$x_1^2+x_2^2+\cdots+x_n^2=0$$

就没有非原点的整点（它只有原点一个整点）。若(d)有实轨迹时，当 $n\geqslant5$，则(d)上有一个非原点的整点，也就是它有无穷多个整点（这是米耶…Meyer…定理，这里不证明）但当 $n=4$时，此定理不成立。如，在

$$x_1^2+x_2^2+x_3^2-7x_4^2=0 \qquad \text{(e)}$$

上没有非原点的整点。若有非原点的整点(x_1,x_2,x_3,x_4)时，可设$(x_1, x_2, x_3, x_4)=1$。因为任何整数x的平方被8除的余数只能是0，1，4三种情况之一出现，又$-7x_4^2$与x_4^2被8除的余数相同，故(e)的左边与

$$x_1^2+x_2^2+x_3^2+x_4^2 \qquad \text{(f)}$$

被8除的余数相等（这些内容在下章引入同余概念后是很简单的）。要(f)被8除的余数为0，只能当x_1，x_2，x_3，x_4）全为偶数时才可以，所以$2|(x_1, x_2, x_3, x_4)$，这与$(x_1, x_2, x_3, x_4)=1$的假设矛盾，故(e)上无整点。

附注：我国古代称直角三角形的两直角边分别为勾与股，斜边为弦。《周髀算经》载有周公与商高的一段问答，其中谈到"句(即勾)广三，股参四，径（即弦）隅五"；而同书中又记载荣方与陈子的问答中谈到从勾股求弦的一般方法是："勾股各自乘，并以开方除之。"一般认为《周髀算经》成书于公元前一世纪，如按周公的年代却是公

元前十一世纪，故这些结论比毕氏学派（公元前六世纪）早500年，毕氏定理的成文记载是在欧氏《几何原本》第一卷第47、48命题给出该定理及其逆定理的证明。

中国的刘徽的九章注（263年）中给出了3，4，5之外的勾股数5，12，13；7，24，25；8，15，17；20，21，29。

古希腊毕氏学派已发现，当m是奇数时，m，$\frac{1}{2}(m^2-1)$，$\frac{1}{2}(m^2+1)$构成勾股弦数。

更早的古巴比仑人在公元前二千年已掌握

$$x=2mn,\ y=m^2-n^2,\ z=m^2+n^2$$

其中m，n都是正整数，m＞n，表示$x^2+y^2=z^2$的一般解

第四节　费马大定理

法国数学家费马（Fermat，1601—1665）大约在1637年左右提出一个猜测：“当整数n＞2时，不定方程

$$x^n+y^n=z^n \tag{16}$$

没有正整数解”．历史上称为费马大定理，或费马猜测，或费马问题。

费马死后，在整理他的书信、文件时发现在巴契（C·G·Bachet de Meziriac,1581—1638)校订的《丢番图》第二卷第8命题“把一个平方数分为两个平方数之和”旁，有费马写的一段批语：“把一个立方数分为两个立方数之和，一个四次幂分为两个四次幂之和，或一般地，把一个高于二次的幂分为两个同次的幂之和，这是不可能的。关于这一点我已发现了一种巧妙的证法，可惜这里空白的地方太小，写不下”．但是，至今为止，数学界仍未得到这一猜测的完整证明。实际上，只需要证明 n＝p 为任一素数时，命题正确就可以了。历史上对这个问题的主要工作情况概述于下：

1770年欧拉证明了 $n=3$，4时，大定理成立。

1678年莱布尼兹（G·W·Leibniz，1646—1716）也证明了 $n=4$ 时大定理成立。

1823年勒让德，1825年狄利克雷（P·G·Lejeune-Dirichlet，1805—1859）分别证明了 $n=5$ 时，大定理成立。

1836年拉美（G·Lame′，1795—1870）证明了 $n=7$ 时，大定理成立。

1844年康米尔（E·E·Kummer）创立了理想数理论，并用它证明了 $2<p<100$ 之间除去 $p=37$，59，67 三数以外的奇素数情况下，大定理成立。

1944年谢尔弗力基、尼可、凡代弗（H·S·Vandiver）证明了 $2<p<4002$ 时，大定理成立。

1976年，瓦格斯塔夫（S·Wagstaff）借助于大型电子计算机证明了 $2<p<125000$ 时，大定理成立。

近来，国外某些数学家，把这个问题转化为用拓扑学知识来解决的问题，降低了该问题的难度，增加了彻底解决问题的可能性。

最近，西德数学家、伍珀塔尔大学讲师法尔廷斯经过十八个月的艰苦努力，对这一问题做出了迄今为止最大的突破，他证实了

$$x^n+y^n=z^n$$

当 $n\geqslant4$ 时，至多只有有限类整数解。法尔廷斯这一工作引起国际数学界的震动，被认为是“本世纪解决的最重要问题”。

下面，我们对这一问题的初等成果作一些简介。

当 $4|n$ 时，(16)式可以写成下列形式：

$$(x^{\frac{n}{4}})^4+(y^{\frac{n}{4}})^4=(y^{\frac{n}{4}})^4$$

所以若能证明：$n=4$时，(16)式没有正整数解，则对于能被4整除的任何正整数n来说，(16)都没有正整数解。因为，若$n=4k$时(16)有正整数解(a,b,c)则$(a^k)^4+(b^k)^4=(c^k)^4$，即(a^k, b^k, c^k)是$x^4+y^4=z^4$的一个正整数解，这与$n=4$时，无正整数解的假设矛盾。

下面我们先证

定理2·6 $x^4+y^4=z^2$ (17)

没有正整数解。

下面无特别声明“解”都指正整数解。

证明 用反证法，若(17)有解，则一定有一个解使得z的值最小，即存在一个最小的正整数u，使得

$$x^4+y^4=u^2,\ x>0,\ y>0,\ u>0 \tag{18}$$

有解，这时$(x, y)=1$，否则，就有$(x, y)>1$且

$$\left(\frac{x}{(x, y)}\right)^4+\left(\frac{y}{(x, y)}\right)^4=\left(\frac{u}{(x, y)}\right)^2,$$

但$0<\dfrac{u}{(x, y)^2}<u$，这与u的最小性矛盾。

其次由前一节的讨论知道，x^2，y^2必定一奇一偶，因此不妨设$2|x^2$，$2\nmid y^2$，由定理2·3得

$$x^2=2ab,\ y^2=a^2-b^2,\ u=a^2+b^2 \tag{19}$$

其中$a>b>0$，$(a, b)=1$，a，b一奇一偶。所以$2|x$，$2\nmid y$，并且$2\nmid a$，$2|b$，因为不然的话，就有$b=2b_1+1$，$a=2a_1$，而$y^2=4(a_1^2-b_1^2-b_1)-1$。另一方面，又有$y=2y_1+1$

$\Longrightarrow y^2=4(y_1^2+y_1)+1$。比较两个结果得

$$4(a_1^2-b_1^2-b_1)-1=4(y_1^2+y_1)+1$$

$$\Longrightarrow 4(a_1^2-b_1^2-b_1-y_1^2-y_1)=2,$$

这是不可能的。于是可设 $b=2c$，得

$$\left(\frac{x}{2}\right)^2=ac,\ (a,\ c)=1.$$

由定理2·3前面的引理2，得

$$a=d^2,\ c=f^2,\ d>0,\ f>0,\ (d,\ f)=1.$$

再由(19)即得

$$y^2=d^4-4f^4\Longrightarrow(2f^2)^2+y^2=(d^2)^2\Longrightarrow(2f^2,\ y)\mid d^2$$
$$且(2f^2,\ d^2)\mid y\Longrightarrow(2f^2,\ y)\mid(2f^2,\ d^2)且$$
$$(2f^2,\ d^2)\mid(2f^2,\ y)\Longrightarrow(2f^2,\ y)=(2f^2,\ d^2)$$
$$=(b,\ a)=1.$$

再由定理2·3，得

$$2f^2=2lm,\ d^2=l^2+m^2,\ l>0,\ m>0,\ (l,\ m)=1.$$

再由前节的引理2，得

$$l=r^2,\ m=s^2,\ r>0,\ s>0$$

代入 $d^2=l^2+m^2$，得

$$r^4+s^4=d^2,\ r>0,\ s>0,\ d>0,$$

而 $d\leqslant d^2=a<a^2+b^2=u$，这与 u 的最小性矛盾，这就证明了所要的定理。

此定理的证明方法是费马所创造的，叫做无穷递降法，其逻辑步骤如下：

(1) 若一命题P(n)对若干正整数 n 为真，则在此诸n中，必有一最小者 n。

(2) 若P(n)为真，则有一正整数 $n'<n$，使P(n′)亦真。若此二步已证，则命题P(n)决不真实。

系 $x^4+y^4=z^4$没有正整数解

用本节开始的讨论方法，知道如果能够再说明对于任一

奇素数 p，(16)都没有正整数解，那末p的任一倍数$kp=n$，(16)也没有正整数解，这样费马大定理就被证明了。

除了一次、二次不定方程之外，不定方程还有丰富的内容，如，在狄克逊（Dickson）所著的数学史第二册中，以六百余页的篇幅来讨论不定方程。早在公元三世纪初，丢番图（Diophantos）就已研究了现在被称为丢番图方程的不定方程，如，$x^2+y^2=z^2$，$x^4+y^4=z^4$，$x^3+y^3=z^3$，$x^3+y^3=3z^3$，$x^3+y^3+z^3=t^3$等等，比起更一般化的费马大定理，历史更加悠久。

习　题

1．求下列不定方程的一切整数解：

(i)　$15x+25y=100$；

(ii)　$253x-449y=1$；

(iii)　$53x+47y=11$；

(iv)　$\{\alpha,\ \beta,\ \gamma,\ \delta\}x-\{\beta,\ \gamma,\ \delta\}y=1$；

(v)　$6x-5y+3z=1$；

(vi)　$5x_1+4x_2-7x_3-3x_4=5$。

2．把100分成两个数之和，使其一是7的倍数，另一是11的倍数。

3．求

$$\begin{cases} 5x+7y+2z=24, & (1)\\ 3x-y-4z=4. & (2)\end{cases}$$

的正整数解。

4．取一分、二分、五分的硬币共十枚，付给一角八分钱，问有几种不同的付法？

5．有布7丈5尺，裁剪成成人和小孩的衣料，大人一件衣服用布7尺2寸，小孩一件衣服用布3尺，问各裁剪多少件衣服，恰好把布用尽？

6. 若N为任意正实数，且$N=N_1+N_2$，$N_1\geqslant 0$，$N_2\geqslant 0$，则

$$[N_1]+[N_2]=\begin{cases}[N],\\ [N]-1.\end{cases}$$

7. 证明，二元一次不定方程

$$ax+by=N,\ (a,\ b)=1,\ a>b>0 \quad (1)$$

的非负整数解的数目为$\left[\frac{N}{ab}\right]$或$\left[\frac{N}{ab}\right]+1$。

8. 证明，二元一次不定方程

$$ax+by=N,\ (a,\ b)=1,\ a>b>1 \quad (2)$$

当$N>ab-a-b$时，有非负整数解，当$N=ab-a-b$时，则不然。

9. 把$\frac{17}{60}$写成分母两两互素的三个既约分数之和。

10. 一百馒头一百僧，大僧三个更无争，小僧三人分一个，大小和尚各几丁？（明程大位《算法统宗》）。

此题并非不定方程的问题，它是有唯一解的线性方程组，其解是大僧25人，小僧75人，若把题目改为：把一百个馒头分给大小和尚，大和尚每人分三个，小和尚三人分一个，问大小和尚各几人？那就是不定方程的问题了。

11. 某地花纱布公司的进货账上，有一笔账被洒上了墨水，变成了下图的样子。如果已知布匹的数量小于100匹，试求出被墨水洒盖的数字（表中打“×”号的是数字）。

品名	数量	单位	单价	金额						
				万	千	百	十	元	角	分
布匹	××	匹	25.3元		×	×	×	5	2	0

12. 勾股数 $3^2+4^2=5^2$可推广于下：

$$(2n^2+n)^2+[2n^2+(n+1)]^2+\cdots+(2n^2+2n)^2$$
$$=[2n^2+(2n+1)]^2+\cdots+(2n^2+3n)^2 \quad (a)$$

n为任意自然数。

13．解不定方程

$$x^2+y^2=z^4. \qquad (1)$$

并证明其解满足

$x>0$，$y>0$，$z>0$，$(x, y)=1$，$2|x$

时，可由下列式子表示之：

$x=4ab(a^2-b^2)$，$y=|a^4+b^4-6a^2b^2|$，$z=a^2+b^2$，

$a>0$，$b>0$，$(a, b)=1$，$a+b$ 被 2 除的余数是1。

14．证明

$$x^4+y^2=z^2,\ 2|x,\ x>0,\ y>0,\ z>0,\ (x, y)=1 \qquad (1)$$

的解答是

$x=2ab$，$y=|4a^4-b^4|$，$z=4a^4+b^4$，$(a,b)=1$，$a>0$，$b>0$

$2\nmid b$。

15．求出 $\sin\theta$，$\cos\theta$ 都是有理数的 θ 值。

16．证明

$$x=\frac{1}{4}[(1+\sqrt{2})^{2n+1}+(1-\sqrt{2})^{2n+1}-2],$$

$$y=\frac{1}{2\sqrt{2}}[(1+\sqrt{2})^{2n+1}-(1-\sqrt{2})^{2n+1}],\ n>0$$

是不定方程

$$x^2+(x+1)^2=y^2 \qquad (\alpha)$$

的解。

17．定出一切边长和面积都是有理数的三角形。

18．证明，不定方程

$$x^4-4y^4=z^2 \qquad (\alpha)$$

无正整数解。

19．证明，定理2·3中方程(11)的解(15)是互素的解。

20．仿照定理2·6的证法，证明

$$x^4+4y^4=z^2 \qquad (1)$$

无正整数解。

21．证明

$$x^4 - y^4 = z^2 \quad (1)$$

无正整数解。

22．已知圆 $x^2+y^2=r^2$（r为奇数），交 x 轴于A(r，0)，B(－r，0)，交 y 轴于C(0，－r)，D(0，r)。P(u，v)是圆周上的一点，$u=p^m$，$v=q^n$（p，q 都是素数，m，n 都是自然数）且 u>v 且 p 在 x 轴和 y 轴上的射影分别是M，N。求证：|AM|，|BM|，|CN|，|DN|分别为1，9，8，2.（1982年联赛试题）。

第三章　同　　余

在日常生活中，我们接触到的不单是某些整数，而且有时是用某一固定的数去除某一数所得的余数。例如，若问现在是几点钟？就是用24去除某一总的时数。若问今天是星期几？就是用 7 去除某一总的天数所得的余数。这样就在数学中产生了同余的概念。

本章主要介绍同余的概念及其基本性质，完全剩余系和互素剩余系，三角和的概念等，并联系中小学实际，把同余的知识应用于对循环小数理论的探讨，以及任意数倍数的判别法等内容

第一节　同余的概念及其性质

例如，已知1982年 5 月 1 日是星期六，问1982年10月 1 日是星期几？

因为 5 月 2 日是星期日，从 5 月 3 日至 5 月31日，还有29天， 6 ， 7 ， 8 ， 9 四个月共有 122 天，加上10月 1 日一天，故从 5 月 3 日至10月 1 日共有$29+122+1=152$(天)，过七天出现一个星期天，而$152=7\times21+5$，所以1982 年 10 月 1 日是星期五。这个例子就可以引出同余的概念，这个概念的产生，大大丰富了数学的内容。

定义3·1　整数 a，b 和正整数 m，若$m\mid(a-b)$，则称 a 和 b 关于模 m 同余（a is congruent to b relative to modulus m）。记作

$$a\equiv b(\bmod m).$$

若$m \nmid (a-b)$，则称 a 和 b 关于模 m 不同余(a is not congruent to b relative to modulus m)。记作

$$a \not\equiv b \pmod m.$$

也就是 a 和 b 被 m 除的余数相同时，称 a 和 b 关于模 m 同余；余数不相同时，a 和 b 关于模m 不同余。

例如，1982年10月1日与5月29日同是星期五，也就是从某日开始计算的总天数，除以7时，它们的余数是相同的，如从5月3日开始的话，就是

$$152 \equiv 5 \pmod 7,\ 26 \equiv 5 \pmod 7 \Longrightarrow 152 \equiv 26 \pmod 7.$$

同余有如下诸性质。

1° 同余关系是一种等价关系，即满足

(i) 反身性：$a \equiv a \pmod m$；

(ii) 对称性：若 $a \equiv b \pmod m$，则 $b \equiv a \pmod m$；

(iii) 传递性：若$a \equiv b$，$b \equiv c \pmod m$，则

$$a \equiv c \pmod m.$$

2° $a_i \equiv b_i \pmod m\ (i=1,2,\cdots,n) \Longrightarrow \sum_{i=1}^{n} a_i \equiv \sum_{i=1}^{n} b_i \pmod m.$

证明 $a_i \equiv b_i \pmod m \Longrightarrow a_i - b_i = k_i m\ (i=1,\cdots,n)$，$k_i$是整数$\Longrightarrow \sum_{i=1}^{n}(a_i-b_i) = \sum_{i=1}^{n} k_i \cdot m \Longrightarrow \sum_{i=1}^{n} a_i - \sum_{i=1}^{n} b_i = Km$。其中$K = \sum_{i=1}^{n} k_i$。由定义3·1，得

$$\sum_{i=1}^{n} a_i \equiv \sum_{i=1}^{n} b_i \pmod m.$$

这个性质包含了

(i) $a_1 \equiv b_1$, $a_2 \equiv b_2 \pmod m \Longrightarrow a_1 \pm a_2 \equiv b_1 \pm b_2$ $\pmod m$;

(ii) $a+b \equiv c \pmod m \Longrightarrow a \equiv c-b \pmod m$.

3° $a_i \equiv b_i \pmod m (i=1,\cdots,n) \Longrightarrow \prod_{i=1}^{n} a_i \equiv \prod_{i=1}^{n} b_i$ $\pmod m$。特别是 $a \equiv b \pmod m \Longrightarrow a^n \equiv b^n \pmod m$.

证明 $a_i \equiv b_i \pmod m \Longrightarrow a_i - b_i = k_i m$

$\Longrightarrow a_i = b_i + k_i m (i=1, \cdots, n)$

$\Longrightarrow a_1 \cdots a_n = b_1 \cdots b_n + Km$.

其中$K = \sum_{r=1}^{n} b_1 \cdots b_{r-1} b_{r+1} \cdots b_n k_r + \sum_{j>i=1}^{n-1} b_1 \cdots b_{i-1} b_{i+1} \cdots$

$b_{j-1} b_{j+1} \cdots b_n \cdot k_i k_j m + \cdots + \sum_{i=1}^{n} b_i k_1 \cdots k_{i-1} k_{i+1} \cdots$

$k_n m^{n-2} + k_1 \cdots k_n m^{n-1}$. 是整数。

$\therefore \quad \prod_{i=1}^{n} a_i \equiv \prod_{i=1}^{n} b_i \pmod m$

当$a_1 = \cdots = a_n = a$, $b_1 = \cdots = b_n = b$ 时，有

$$a^n \equiv b^n \pmod m.$$

一般地

4° $a_i \equiv b_i \pmod m$ $(i=0,1,\cdots,n)$, $x \equiv y \pmod m$

$\Longrightarrow a_0 + a_1 x + \cdots + a_n x^n \equiv b_0 + b_1 y + \cdots + b_n y^n$

$\pmod m$.

这个结论还可以推广到多元多项式

5° $a \equiv b \pmod m$, $k > 0 \Longrightarrow ak \equiv bk \pmod{mk}$.

证明 $a = b + mt \Longrightarrow ak = bk + mkt \Longrightarrow ak \equiv bk$

$\pmod{mk}$.

6° $a \equiv b \pmod m$, $d \mid (a,b,m) \Longrightarrow \frac{a}{d} \equiv \frac{b}{d}\left(\bmod \frac{m}{d}\right)$

7° $a \equiv b \pmod m$, $d \mid (a, b)$且$(d,m)=1$

$\Longrightarrow \frac{a}{d} \equiv \frac{b}{d} \pmod m$.

8° $a \equiv b \pmod m$, $d>0$, $d \mid m \Longrightarrow a \equiv b \pmod d$.

9° $a \equiv b \pmod m \Longrightarrow (a, m)=(b, m)$.

换言之，若 d 整除 m 及 a，b 中的一个时，则 d 整除 a，b 中的另一个数。

10° $(a, m)=1$, $ax \equiv ay \pmod m \Longrightarrow x \equiv y \pmod m$.

此性质实际是性质7°的另一种形式。

11° $a \equiv b \pmod{m_i} (i=1, \cdots, k)$

$\Longrightarrow a \equiv b (\bmod [m_1, \cdots, m_k])$.

以上诸性质，留给读者自行证明。

例3·1 用a_0，a_1，…，a_n表示$n+1$位数的各位数字，即

$$a=a_n 10^n+a_{n-1} 10^{n-1}+\cdots+a_1 10+a_0 (0 \leqslant a_i \leqslant 9, \ i=0, 1, \cdots, n, a_n \neq 0).$$

因为$10 \equiv -1 \pmod{11}$，所以由性质4°得

$$a \equiv (-1)^n a_n+(-1)^{n-1} a_{n-1}+\cdots+(-1) a_1+a_0 \pmod{11} \Longleftrightarrow a \equiv (a_0+a_2+\cdots)-(a_1+a_3+\cdots) \pmod{11}$$

于是得到一种判别一个正整数 a 是否11的倍数的判别法：奇位（个位、百位、万位等等）数字之和，减去偶位（十位、千位、十万位等等）数字之和的差，若是11的倍数，则 a 亦是11的倍数；“差”若不是11的倍数，则 a 亦不是11的倍数。

同理，因为$10 \equiv 1 \pmod 9$，$10 \equiv 1 \pmod 3$，所以

$$9|a \Longleftrightarrow 9|a_0+a_1+\cdots+a_n;$$

$$3|a \Longleftrightarrow 3|a_0+a_1+\cdots+a_n.$$

一般地，检查一个数 d 是否另一个数 a 的因数的方法，是构造一个函数 f(a)，使它满足下列三条原则：

(i) a 和 f(a)同时能被 d 整除，或者同时不能被 d 整除，即

$$d|f(a) \Longleftrightarrow d|a.$$

(ii) 除了 a 充分小之外，总有$|f(a)|<|a|$

(iii) 对于已知 a，f(a)计算起来比较简单。

例3·2 设

$a=a_n 1000^n+a_{n-1}1000^{n-1}+\cdots+a_1 1000+a_0$，

$0\leqslant a_i<1000$，$a_n\neq 0$，n是非负整数。

∵ $1000\equiv -1(\bmod 7)$[或$(\bmod 11)$或$(\bmod 13)$]，

令 $f(a)=(a_0+a_2+\cdots)-(a_1+a_3+\cdots)$，则

$7|a \Longleftrightarrow 7|f(a)$[或$11|a \Longleftrightarrow 11|f(a)$，或

$13|a \Longleftrightarrow 13|f(a)$]。

一、巴斯加（Pascal）法

在十进位计数法中，任一自然数 a 都可以表成：

$$a=a_n 10^n+a_{n-1}10^{n-1}+\cdots+a_1 10+a_0$$

$$(0\leqslant a_i\leqslant 9,\ a_n\neq 0) \tag{1}$$

本节下面所指的 a，都是(1)形式的整数。

要判别自然数 d 是否整除 a，可依据

定理3·1 若$10_k\equiv c_k(\bmod d)$，c_k是绝对值最小的剩余，$k=0,1,\cdots,n$，则 $d|a$ 的充要条件是：d整除

$$f(a)=a_n c_n+a_{n-1}c_{n-1}+\cdots+a_1 c_1+a_0.$$

证明 由性质3° 知道

$$a_n 10^n\equiv a_n c_n,\ a_{n-1}10^{n-1}\equiv a_{n-1}c_{n-1},\cdots,a_1 10\equiv a_1 c_1$$

$$a_0 \equiv a_0 (\mathrm{mod}\ d).$$

由性质2°，得

$$a \equiv f(a) \quad (\mathrm{mod}\ d)$$

∴ $d \mid a \Longrightarrow d \mid f(a)$，$d \nmid a \Longrightarrow d \nmid f(a)$

即 $d \mid a \Longleftrightarrow d \mid f(a)$.

例3·3 (i) $d=2$，$c_k=0$，$(k=1,2,\cdots)$，所以 $a \equiv a_0(\mathrm{mod}2)$。这是大家所熟悉的，若a的个位数字是偶数，则$2 \mid a$；否则$2 \nmid a$。

(ii) $d=4$，$c_1=\pm 2$，$c_2=c_3=\cdots=c_n=0$，所以 $a \equiv a_0 \pm 2a_1(\mathrm{mod}4)$。即

$$4 \mid a \Longleftrightarrow 4 \mid a_0 \pm 2a_1.$$

(iii) $d=6$，$c_1=c_2=\cdots=c_n=-2$，所以

$$6 \mid a \Longleftrightarrow 6 \mid a_0-2(a_1+a_2+\cdots+a_n).$$

(iv) $d=7$，$c_1=3$，$c_2=2$，$c_3=-1$，$c_4=-3$，$c_5=-2$，$c_6=1$，$c_7=3$，$c_8=2$，$\cdots$，所以

$$a \equiv (a_0+3a_1+2a_2)-(a_3+3a_4+2a_5)+(a_6+3a_7+2a_8)\cdots(\mathrm{mod}7)$$

如，$637693 \equiv (3+3\times 9+2\times 6)-(7+3\times 3+2\times 6)=14 \equiv 0(\mathrm{mod}7)$.

∴ $7 \mid 637693$.

(v) $d=8$，$c_1=2$，$c_2=\pm 4$，$c_3=c_4=\cdots=c_n=0$，所以

$$a \equiv a_0+2a_1 \pm 4a_2(\mathrm{mod}8).$$

如，$a=637174 \equiv 4+2\times 7-4=14 \equiv 6(\mathrm{mod}8)$

∴ $8 \nmid 637174$.

(vi) $d=11$，$c_k=(-1)^k(k=1,2,\cdots,n)$，所以

$$a \equiv (a_0+a_2+a_4+\cdots)-(a_1+a_3+\cdots)(\mathrm{mod}11).$$

如，$1584 \equiv (4+5)-(8+1)=0 \pmod{11}$

$\therefore \quad 11 \mid 1584$。

(vii) $d=5$，$c_k=0\ (k=1, 2, \cdots, n)$，所以

$$a \equiv a_0 \pmod 5$$

(viii) $d=25$，$c_1=10$，$c_2=\cdots=c_n=0$，所以

$$25 \mid a \Longleftrightarrow 25 \mid a_1 \times 10 + a_0。$$

二、日比可夫斯基（А·К·Жбиковский）法

当$(10, d)=1$时，不定方程

$$10x+dy=a \qquad (2)$$

对于任意整数 a，都有整数解(x_0, y_0)，一般解是

$$x=x_0-dt, \quad y=y_0+10t \quad (t=0, \pm 1, \pm 2, \cdots)。$$

所以 $x \equiv x_0 \pmod d$的任一 x 值，都是

$$10x \equiv a \pmod d$$

的解。即$10x_0 \equiv a \pmod d$，可选取 x_0是 x 关于模 d 的最小非负剩余($0 \leqslant x_0 < d$)或绝对最小剩余($0 \leqslant |x_0| \leqslant \frac{d}{2}$)，并且有

(i) 若$x_0=0$，则 $d \mid a$，即$d \mid x \Longrightarrow d \mid a$；

(ii) 若$x_0 \neq 0$，则$d \nmid a$，即$d \nmid x \Longrightarrow d \nmid a$。

我们取 $f(a)=x_0$，先解$10k+dy=1$，即求出满足$10k \equiv 1 \pmod d$的整数k，那末

$$10ka_1 \equiv a_1 \pmod d。$$

而

$$ka = ka_0 + 10ka_1 + 10k \cdot 10a_2 + \cdots + 10k \cdot 10^{n-1}a_n$$
$$\equiv (ka_0+a_0) + 10a_2 + \cdots + 10^{n-1}a_n \pmod d，$$

所以，我们取

$$f(a)=(ka_0+a_1)+10a_2+\cdots+10^{n-1}a_n,$$

则 $\quad d \mid a \Longleftrightarrow d \mid f(a)。$

这样的 f(a)比 a 少了一位，此法亦称划尾法。上述的分析已经证明了

定理3·2 若$(d,\ 10)=1$，k 是满足$10k\equiv 1 \pmod d$的整数，并且$0\leqslant |k| \leqslant \frac{d}{2}$，则

$$d|a \Longleftrightarrow d|f(a)$$

其中$f(a)=(ka_0+a_1)+10a_2+\cdots+10^{n-1}a_n$。

注意：由定理3·2所定义的 f(a)，一般$f(a)\not\equiv a \pmod d$

例3·4 (i) $d=3$，当$k=1$时，$10k\equiv 1 \pmod 3$（这样$k\equiv 1 \pmod 3$的 k 叫做$10k\equiv 1 \pmod 3$的一个解，下同），所以

$$f(a)=(a_0+a_1)+10a_2+\cdots+10^{n-1}a_n。$$

如，判别187562431是否3的倍数，可用划尾法：

$187562431\longrightarrow 18756240+(3+1)=18756244\longrightarrow 1875628\longrightarrow 187570\longrightarrow 1882\longrightarrow 190$

$\therefore\quad 3\nmid 187562431$。

(ii) $d=7$，$10k\equiv 1 \pmod 7$有解$k=-2$（或$k=5$）所以

$f(a)=(a_1-2a_0)+10a_2+\cdots$

（或$f(a)=(a_1+5a_0)+10a_2+\cdots$）。

如，$a=637693\to 63763\to 6370\to 49$

$\therefore\quad 7|637693$。

(iii) $d=11$，则$k=-1$，$f(a)=(a_1-a_0)+10a_2+\cdots$。

如，$13678511\to 1367850\to 13673\to 1364\to 132\to 11$。

$\therefore\quad 11|13678511$。

(iv) $d=13$，则$k=4$，$f(a)=(a_1+4a_0)+10a_2+\cdots$

如，$3918231\to 391827\to 39210\to 396\to 63$

∴　$13 \nmid 3918231$

(v)　$d=17$，则$k=-5$，$f(a)=(a_1-5a_0)+10a_2+\cdots$

如，$a=63785343 \to 6378519 \to 637806 \to 63750 \to 612 \to 51$

∴　$17 \mid 63785343$。

三、逆除法

因为用与10互素的末位数字（即1，3，7，9）来乘作为个位数字的数列0，1，2，…，9的各项，乘积的个位数字仍然是0，1，…，9的一个排列。如，$7\times0=0$，$7\times1=7$，$7\times2=14$，$7\times3=21$，$7\times4=28$，$7\times5=35$，$7\times6=42$，$7\times7=49$，$7\times8=56$，$7\times9=63$。积的个位数字依次是：0，7，4，1，8，5，2，9，6，3．又因$(d,10)=1$的d的末位数字一定是1，3，7，9之一，于是可用划尾法的精神，把要判别是否是d的倍数的整数a减去一个d的倍数，使这个倍数的末位数字与a的末位数字相同，此法称为逆除法．例如，判别546是否7的倍数时，可用

```
5 4 6|7
  5 6|7 8
4 9
4 9
  0
```

∴　$7 \mid 546$。

亦即　$546 \to 546-56=490$，∴$7 \mid 546$。

又如，问42315能否被13整除？

$42315 \to 42315-65=42250 \to 4225-65=4160 \to 39$

∴　$13 \mid 42315$。

最后，介绍一种验算正整数计算结果的方法—弃九法。

设我们用普通乘法，求出二整数a和b之积P，令

$a=10^n a_n+\cdots+10a_1+a_0$（$0\leqslant a_i\leqslant9$）；

$$b = 10^m b_m + \cdots + 10b_1 + b_0 \ (0 \leqslant b_j \leqslant 9);$$

$$= ab$$

$$P = 10^l c_l + \cdots + 10c_1 + b_0 \ (0 \leqslant c_k \leqslant 9).$$

由于$10^k \equiv 1 \pmod 9$，由性质4°得

$$a \equiv \sum_{i=D}^{n} a_i, \quad b \equiv \sum_{j=o}^{m} b_j, \quad P \equiv \sum_{k=o}^{l} c_k \pmod 9.$$

所以，若

$$\sum_{i=D}^{n} a_i \sum_{j=0}^{m} b_j \equiv \sum_{k=0}^{l} c_k \pmod 9 \qquad (3)$$

成立，则$P = ab$的可能性很大。若（3）不成立，则$P \neq ab$，即计算肯定是错误的。必须注意，（3）成立并非计算绝对无误。

定理3·3 如果$ab = P$的计算无误，那末同余式（3）必成立。

例3·5 设$a = 28997$，$b = 39495$，若$ab = P = 1145236415$。问乘法是否有误？

解：∵ $a \equiv 8$，$b \equiv 3$，$P \equiv 5 \pmod 9$

而 $8 \times 3 \equiv 6 \not\equiv 5 \pmod 9$，

所以计算是错误的。

必须再次强调，（3）成立仅是$P = ab$计算无误的必要条件，非充分条件。如，例3·5的正确结果是：$P = 1145236515$，若计算结果是$P = 1145235615$，则用弃九法计算得$P \equiv 6 \pmod 9$，$8 \times 3 \equiv 6 \pmod 9$，这时不能就说$a \times b = 1145235615$是对的，只能说计算对的可能性较大。

"弃九"指的是a，b，P的数字之和"遇九即弃"的意义，如，$2+8+9+9+7-3\times 9 = 8$（弃去三个九）；

$3+4+5+6+7+2+3-3\times 9=3$ 等等。

第二节　剩余类与完全剩余系

上节引入了同余（congruence）的概念，由于带余除法余数的唯一性，因此任意整数a，被自然数m除所得的余数一定是：0，1，2，…，m-1中的一个，并且只有一个是它的余数。因此，把余数相等的一切整数放在一起，构成一个"类"，这样

（i）每一个整数都属于一个类，且仅属于一个类；

（ii）两个整数a和b属于同一类的充分且必要条件是：$a\equiv b\pmod m$。

定理3·4　若给定了自然数m，则全部整数可以分成m个集合，这样的集合叫做类（class）。并记作：{0}，{1}，{2}，…，{m-1}，其中类{r}（r=0，1，…，m-1）是由一切形如 $a=qm+r$（$q=0，\pm1，\pm2，\cdots$）的整数a所组成。则，这些类具有下列性质：

1．每一个整数必属于这m个类中的一个，且仅属于一个。

2．两个整数a和b属于同一类的充要条件是：$a\equiv b\pmod m$。

定理前面的分析，实际已证明了上面定理。

定义3·2　定理3·4中的{0}，{1}，…，{m-1}叫做模m的剩余类（residue class of modulus m，or，class of residues(modm)）。一个剩余类中的任一数，叫做这个类的代表（repreesentation）或剩余（residue）。若a_0，a_1，…，a_{m-1}是m个整数，并且其中二数都不同在一

个剩余类里，则a_0，a_1，…，a_{m-1}的全体，叫做模m的一个全体代表团（a complete representative system of incongruent residues to modulus m），或称模m的一个完全剩余系（a complete system of incongruent residues to modulus m，或简写为a complete system (mod m)），简称完全剩余系．

由定理3·4立即得到：

系 m个整数形成一个模m的完全剩余系的充要条件是．它们之间两两对模m互不同余．

由系，我们知道

$$0，1，2，\cdots，m-1; \tag{a}$$

$$0，m+1，\cdots，rm+r，\cdots，(m-1)m+(m-1); \tag{b}$$

$$0，-m+1，\cdots，(-1)^r m+r，\cdots，(-1)^{m-1}m+(m-1) \tag{c}$$

等等，都是模m的完全剩余系．

当m是偶数时，

$$-\frac{m}{2}，-\frac{m}{2}+1，\cdots，-1，0，1，\cdots，\frac{m}{2}-1; \tag{d}$$

$$-\frac{m}{2}+1，\cdots，-1，0，1，\cdots，\frac{m}{2}-1，\frac{m}{2} \tag{d)'$$

当m是奇数时，

$$-\frac{m-1}{2}，\cdots，-1，0，1，\cdots\frac{m-1}{2} \tag{e}$$

亦都是模m的完全剩余系。

其中(a)称为模m的非负最小完全剩余系，(a)中的每一个数都叫做模m的非负最小剩余。(d)，(d)′和(e)叫做模m的绝对最小完全剩余系，其中的每一个数都叫做模m的绝对最小剩余。由整除的性质9°知道，若$(r, m)=1$，则$(km+r, m)=1$，即类$\{r\}$中任意一个数都与m互素，我们把这样的类$\{r\}$叫做与模m互素的剩余类。

定义3·3 欧拉函数$\varphi(m)$（Euler′s function $\varphi(m)$）是对于任一自然数都有意义的函数，对给定的自然数m，它的函数值，等于序列0，1，…，$m-1$中与m互素的数的个数。

如果模m的剩余类中的每一个数都与m互素，则称它为与模m互素的剩余类。

在每一个与模m互素的剩余类中，各取一个代表，构成一个代表团，这个代表团称为一个与模m互素的剩余系，简称互素剩余系（complete set of residue prime），或称模m的简化剩余系（reduced residue system to modulus m）。

显然与模m互素的剩余类的个数是$\varphi(m)$，所以模m的互素剩余系中包含有$\varphi(m)$个剩余

$$a_1, \ a_2, \ \cdots, \ a_{\varphi(m)} \tag{f}$$

其中$(a_i, m)=1$（$i=1, \cdots, \varphi(m)$），并且当$i\neq j$时

$$a_i \not\equiv a_j \pmod{m}.$$

定理3·5 若$(a, m)=1$，b是任意整数，则在$ax+b$中，当变数x通过模m的完全剩余系时，$ax+b$亦通过模m的完全剩余系。

证明 假设x过（即通过）完全剩余系

$$a_1,\ a_2,\ \cdots,\ a_m$$

而 $b_i = aa_i + b\ (i = 1,\ 2,\ \cdots,\ m)$，

$(a,\ m) = 1$。

今证明b_1，b_2，…，b_m亦完全剩余系．事实上，只需证它们两两互不同余就可以了，$i \neq j$时，若

$$aa_i + b \equiv aa_j + b\ (\mathrm{mod}\ m) \Longrightarrow aa_i \equiv aa_j\ (\mathrm{mod}\ m)$$

$$\overset{(a,\ m)}{\underset{10。}{\Longrightarrow}} a_i \equiv a_j\ (\mathrm{mod}\ m)$$

这与a_1，…，a_m是模m的完全剩余系的假设矛盾

$$\therefore\quad aa_i + b \not\equiv aa_j + b\ (\mathrm{mod}\ m).$$

系 1 若二正整数m_1，m_2，且$(m_1,\ m_2) = 1$，而x_1，x_2分别过模m_1，m_2的完全剩余系，则$m_2x_1 + m_1x_2$过模m_1m_2的完全剩余系。

证明 当x_1，x_2分别过模m_1，m_2的完全剩余系时，$m_2x_1 + m_1x_2$共有m_1m_2个整数，今证明它们互不同余。否则，若

$$m_2x_1' + m_1x_2' \equiv m_2x_1'' + m_1x_2''\ (\mathrm{mod}\ m_1m_2) \qquad (a)$$

其中x_1'，x_1''；x_2'，x_2''分别取值于模m_1，m_2的完全剩余系。移项得

$$m_2(x_1' - x_1'') \equiv m_1(x_2'' - x_2')$$

$(\mathrm{mod}\ m_1m_2)$。

由同余的性质9°知道，$m_2 \mid m_1(x_2'' - x_2')$，$m_1 \mid m_2(x_1' - x_1'')$而$(m_1,\ m_2) = 1$，所以$m_2 \mid (x_2'' - x_2')$，

$m_1 | (x_1' - x_1'')$

$$\therefore \quad x_1' \equiv x_1'' \pmod{m_1}, \quad x_2' \equiv x_2'' \pmod{m_2}$$

这证明了当x_1'，x_2'与x_1''，x_2''不全相同时(a)不成立。故定理得证。

系 2　若$(a, m) = 1$，x过模m的互素剩余系，则ax亦过模m的互素剩余系。

证明　假设x过与模m互素的剩余系

$$a_1, \ a_2, \ \cdots, \ a_{\varphi(m)},$$

令$b_i = aa_i (i = 1, 2, \cdots, \varphi(m))$。今证明

(i)　$(b_i, m) = 1 \ (i = 1, \cdots, \varphi(m))$。事实上，$(b_i, m) = (aa_i, m)$，因为$(a, m) = 1$，所以

$$(b_i, m) = (a_i, m) = 1.$$

(ii)　当$i \neq j$时，$b_i \not\equiv b_j \pmod{m}$。否则，若$aa_i \equiv aa_j \pmod{m}$，因$(a, m) = 1$，得

$$a_i \equiv a_j \pmod{m}.$$

与a_i，a_j不属于同一类的假设矛盾。

系 3　若m_1，m_2是两个互素的正整数，x_1与x_2分别过模m_1，m_2的互素剩余系，则$m_2 x_1 + m_1 x_2$过模$m_1 m_2$的互素剩余系。

证明　因为模m的一个互素剩余系，是从一个模m的完全剩余系中取出一切与m互素的剩余组成的。因此只需证明：若x_1，x_2分别过模m_1，m_2的互素剩余系，则$m_2 x_1 + m_1 x_2$过模$m_1 m_2$完全剩余系中的一切与模$m_1 m_2$互素的剩余由系 1 知道它们是两两互不同余的，故只需证明：

(i)　当$(x_1, m_1) = 1$，$(x_2 m_1) = 1$且(m_1, m_2)

$=1$ 时，就有，$(m_2x_1+m_1x_2, m_1m_2)=1$；

(ii) $\forall(m_2x_1+m_1x_2, m_1m_2)=1$，且$(m_1, m_2)=1$，都有，$(x_1, m_1)=1$ 且$(x_2, m_2)=1$．

事实上，(i)若

$(x_1, m_1)=1$，$(x_2, m_2)=1$，且$(m_1, m_2)=1$

$\Longrightarrow(m_2x_1, m_1)=1$，且$(m_1x_2, m_2)=1$

$\Longrightarrow(m_2x_1+m_1x_2, m_1)=1$，

且$(m_2x_1+m_1x_2, m_2)=1$

$\Longrightarrow(m_2x_1+m_1x_2, m_1m_2)=1$．

(ii) $\forall(m_2x_1+m_1x_2, m_1m_2)=1$ 且$(m_1, m_2)=1$

$\Longrightarrow(m_2x_1+m_1x_2, m_1)=1$，

且$(m_2x_1+m_1x_2, m_2)=1$

$\Longrightarrow(m_2x_1, m_1)=1$，且$(m_1x_2, m_2)=1$ 又因

$(m_1, m_2)=1$

$\Longrightarrow(x_1, m_1)=1$，且$(x_2, m_2)=1$．

由系 3 立即得到

系 4 若$(m_1, m_2)=1$，则 $\varphi(m_1m_2)=\varphi(m_1)\varphi(m_2)$．

证明 由系 3 知道，若x_1，x_2分别过模m_1，m_2的互素剩余系，则$m_2x_1+m_1x_2$共有$\varphi(m_1)\varphi(m_2)$个剩余，它们刚好过模m_1m_2的互素剩余系．故其数目是$\varphi(m_1m_2)$．

$\therefore\quad \varphi(m_1m_2)=\varphi(m_1)\varphi(m_2)$．

定理3·6 设$m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$，则

$$\varphi(m)=m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right).$$

证明 由定理3·5的系 4 知

$$\varphi(m)=\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\cdots\varphi(p_k^{\alpha_k}).$$

今证明$\varphi(p^\alpha)=p^\alpha-p^{\alpha-1}$。事实上，由$\varphi(a)$的定义知，$\varphi(p^\alpha)$等于从$p^\alpha$减去1，2，…，$p^\alpha$中减去素数p的倍数的个数．由第一章中函数[x]的性质(vii)知，1，2，…，p^α中被p整除的数的个数是$\left[\frac{p^\alpha}{p}\right]=p^{\alpha-1}$.所以

$$\varphi(p^\alpha)=p^\alpha-p^{\alpha-1}=p^\alpha\left(1-\frac{1}{p}\right),$$

$$\therefore\quad \varphi(m)=p_1^{\alpha_1}\left(1-\frac{1}{p_1}\right)p_2^{\alpha_2}\left(1-\frac{1}{p_2}\right)\cdots p_k^{\alpha_k}\left(1-\frac{1}{p_k}\right)=m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right).$$

系 1 $\varphi(1)+\varphi(p)+\cdots+\varphi(p^\alpha)=p^\alpha$，其中p是素数。

证明 因为$\varphi(p^k)=p^k-p^{k-1}$，$(k=1,2,\cdots,\alpha)$，所以

$$\varphi(1)+\varphi(p)+\cdots+\varphi(p^\alpha)=1+(p-1)+(p^2-p)+\cdots+(p^\alpha-p^{\alpha-1})=p^\alpha$$

系 2 $\sum_{d|m}\varphi(d)=m$，其中$\sum_{d|m}$表示展布在m的一切正因数上的和式。

证明 设$m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$，则

$$\sum_{d|m}d=(1+p_1+\cdots+p_1^{\alpha_1})(1+p_2+\cdots+p_2^{\alpha_2})\cdots(1+p_k+\cdots+p_k^{\alpha_k}),$$

$$\therefore \sum_{d|m}\varphi(d)=\left(1+\varphi(p_1)+\cdots+\varphi(p_1^{\alpha_1})\right)\left(1+\varphi(p_2)+\cdots+\varphi(p_2^{\alpha_2})\right)\cdots\left(1+\varphi(p_k)+\cdots+\varphi(p_k^{\alpha_k})\right)$$

$$=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}=m.$$

第三节　欧拉定理、费马定理及其对循环小数的应用

本节应用互素剩余系的性质来证明数论中两个著名的定理，并说明它在研究循环小数时的应用。

定理3·7　欧拉定理(Euler's theorem)，设 m 是大于1的整数，$(a,\ m)=1$，则

$$a^{\varphi(m)}\equiv 1\ (\mathrm{mod}\ m).$$

证明　设 $r_1,\ r_2,\ \cdots,\ r_{\varphi(m)}$ 是模m的互素剩余系，当 $(a,\ m)=1$ 时，由定理3·5的系2知，$ar_1,\ ar_2,\ \cdots,\ ar_{\varphi(m)}$ 也是模m的互素剩余系，所以

$$(ar_1)(ar_2)\cdots(ar_{\varphi(m)})\equiv r_1r_2\cdots r_{\varphi(m)}\ (\mathrm{mod}\ m),$$

即　$a^{\varphi(m)}r_1r_2\cdots r_{\varphi(m)}\equiv r_1r_2\cdots r_{\varphi(m)}\ (\mathrm{mod}\ m)$，

但 $(r_1,\ m)=(r_2,\ m)=\cdots=(r_{\varphi(m)},\ m)=1$

$$\Longrightarrow (r_1\cdots r_{\varphi(m)},\ m)=1,$$

由第一节的性质10°，得

$$a^{\varphi(m)}\equiv 1\ (\mathrm{mod}\ m).$$

当 $m=p$ 为素数时，$\varphi(p)=p-1$，故得

系1　费马定理(Fermat's theorem)，设 p 为素数，$(p,\ a)=1$，则

$$a^{p-1}\equiv 1\ (\bmod\ p).$$

系 2　设p为素数，对于任意整数a，都有

$$a^{p}\equiv a\ (\bmod\ p).$$

如果把含有变数x的同余式（congruence）看作是定义在模m的剩余类集合上的"方程"，通常称这种方程为同余方程（congruent equation）。例如，$x^{\varphi(m)}\equiv 1\ (\bmod m)$有$\varphi(m)$个解；$x^{p-1}\equiv 1\ (\bmod p)$有$\varphi(p)=p-1$个解；$x^{p}\equiv x\ (\bmod p)$有p个解。事实上，这些方程的系数和解，都是模m（或p）的剩余类。

例3·6　如果今天是星期1，问从今天起再过$10^{10^{10}}$天是星期几？

解　若$10^{10^{10}}+1$被7除的非负最小剩余是r，则这一天就是星期r（当r＝0时是星期日）。因为$(10,7)=1$，由费马定理知，$10^{k\times 6}\equiv 1\ (\bmod 7)$，所以可先求$10^{10}\equiv a\ (\bmod 6)$的a，即$(-2)^{10}\equiv a(\bmod 6)$。而$(-2)^{10}=4^{5}\equiv 4\ (\bmod 6)$，即$10^{10}=6k+4$。

$\therefore\ 10^{10^{10}}+1=10^{6k+4}+1\equiv 10^{4}+1\equiv 3^{4}+1\equiv 5\ (\bmod 7)$。

答：该天是星期五。

欧拉定理和费马定理在数论中是很有用的，下面说明它在分数与小数互化中的作用。

任何一个有理数，都可以写成分数$\frac{a}{b}(b>0)$的形式，并由带余除法知，$a=bq+r,\ 0\leqslant r<b$，

即

$$\frac{a}{b}=q+\frac{r}{b},\quad c\leqslant\frac{r}{b}<1.$$

所以我们只要讨论0与1之间的分数与小数互化的问题，就可以了。

定义3·4 如果对于一个无限小数

$$0.a_1a_2\cdots a_n\cdots(0\leqslant a_i\leqslant 9;i=1,2,\cdots,n,\cdots)\tag{4}$$

从任何一位之后不全为0，能够找到两个整数$s\geqslant 0$，$t>0$，使得

$$a_{s+i}=a_{s+kt+i}(i=1,2,\cdots,t;k=0,1,2,\cdots)$$

则称(4)为循环小数(recurring decimal)，并简单地记作

$$0.a_1\cdots a_s\dot{a}_{s+1}\cdots\dot{a}_{s+t}$$

对循环小数而言，具有上述性质的s及t是不只一个的，如果找到的t是最小的，我们就称$a_{s+1}\cdots a_{s+t}$为循环节(recurring period)；t称为循环节的位数(digits)或长度(length)).若最小的$s=0$，则这个循环小数叫做纯循环小数(pure recurring decimal)；否则，若$s>0$，则该小数叫做混纯环小数(mixed recurring decimal)。

例如，$\frac{1}{3}=0.333\cdots=0.\dot{3}$，$\frac{1}{7}=0.\dot{1}4285\dot{7}$都是纯循环小数，前者循环节长为1，后者为6.

定理3·8 有理数$\frac{a}{b}$，$0<a<b$，$(a,b)=1$，能表成纯循环小数的充分且必要条件是：$(b,10)=1$。

证明 (i) 若$\frac{a}{b}=0.\dot{a}_1\cdots\dot{a}_t$为纯循环小数，则

$$10^t\frac{a}{b}=10^{t-1}a_1+\cdots+10a_{t-1}+a_t+0.\dot{a}_1\cdots\dot{a}_t$$

$$=q+\frac{a}{b}\quad (=a_1\cdots a_t q>0).$$

$$\therefore\quad a(10^t-1)=bq$$

由于$(a, b)=1$，所以$b|10^t-1\Longrightarrow(b, 10)=1$。这就证明了条件的必要性。

(ii) 若$(b, 10)=1$，由定理3·7知，存在一个正整数t，使得

$$10^t\equiv 1\ \left(\bmod b\right)\ \left(0<t\leqslant\varphi(b)\right).$$

成立，因此

$$10^t=kb+1\Longrightarrow\frac{10^t}{b}=k+\frac{1}{b}>1\Longrightarrow(10^t-1)\frac{a}{b}$$

$$=ka=q,\quad 0<\frac{a}{b}<1\Longrightarrow 0<q<10^t-1.$$

$$\therefore\quad q=a_1a_2\cdots a_t\left(0\leqslant a_i\leqslant 9\ (i=1, 2, \cdots, t)\right)$$

其中a_1，a_2，…，a_t不全为9亦不全为0。又因

$$10^t\frac{a}{b}=q+\frac{a}{b},\quad \frac{q}{10t}=0.a_1a_2\cdots a_t,$$

$$\therefore\quad \frac{a}{b}=0.a_1\cdots a_t+\frac{1}{10^t}\frac{a}{b}=0.a_1\cdots a_ta_1\cdots a_t$$

$$+\frac{1}{10^{2t}}\cdot\frac{a}{b},$$

重复上面的演算，即得

$$\frac{a}{b}=0.a_1\cdots a_ta_1\cdots a_t\cdots a_1\cdots a_t\cdots=0.\dot{a}_1\cdots\dot{a}_t$$

这就证明了定理的充分性。

系1 若$\frac{a}{b}$是有理数，其中$0<a<b$，$(a, b)=1$，$b=2^\alpha 5^\beta b_1$，$(b_1, 10)=1$，$b_1>1$，α，β不全为0，则$\frac{a}{b}$可以

表成混循环小数，其中不循环的位数是：$u=\max(\alpha, \beta)$（即α、β中大的一个）。

证明 不失一般性，可设$u=\beta\geqslant\alpha$，用10^u乘$\frac{a}{b}$得

$$10^u\frac{a}{b}=\frac{2^{\beta-\alpha}a}{b_1}=M+\frac{a_1}{b_1},\quad 0<a_1<b_1$$

其中$(a_1, b_1)=1$，$(b_1, 10)=1$，$0\leqslant M<10^u$。事实上，由带余除法得

$$2^{u-\alpha}a=Mb_1+a_1,\quad 0<a_1<b_1.$$

因为$(a,b)=1\Longrightarrow(a, b_1)=1$，又$(2^{u-\alpha}, b_1)=1$
$\Longrightarrow 1=(2^{u-\alpha}a, b_1)=(Mb_1+a_1, b_1)=(a_1, b_1)$。

由定理3·8知

$$\frac{a_1}{b_1}=0.\dot{c}_1\cdots\dot{c}_t,$$

且 $M=10^u\frac{a}{b}-\frac{a_1}{b_1}<10^u\frac{a}{b}<10^u$，故设

$$M=m_1 10^{u-1}+\cdots+M_u\ (0\leqslant m_j\leqslant 9,$$
$j=1, \cdots, u)$

$$\therefore\quad \frac{a}{b}=0.m_1\cdots m_u\dot{c}'_1\cdots c'_{t'}$$

最后，还要证明，不循环的位数不能小于u，假定$\frac{a}{b}$又可表成

$$\frac{a}{b}=0.m'_1\cdots m'_v\dot{c}'_1\cdots\dot{c}'_{t'}\ (v<u).$$

则由定理3·8的证明过程中，知道

$$10^v\frac{a}{b}-\left[10^v\frac{a}{b}\right]=0.c'_1\cdots c'_{t'}=\frac{a'_1}{b'_1}$$

$$\left((b_1,10)=1\right).$$

$$\therefore\quad 10^v\frac{a}{b}=\frac{a_1'}{b_1'}+\left[10^v\frac{a}{b}\right]=\frac{a'}{b_1'}\Longrightarrow 10^v a b_1'=a'b.$$

上式右边被$5^\beta=5^u$除尽，而左边a及b_1'都与5互素

$\left(\because (a,b)=1,\ (b_1',10)=1\right)$，故$5^u\mid 10^v\Longrightarrow u\geqslant v$，

这与$v<u$的假设矛盾。

第四节　三角和

本节将最简单地介绍，近代数论中很重要的方法之一——三角和方法。

在第二节中讲过，模m的剩余类有m个：$k_0=\{0\}$，$k_1=\{1\}$，…，$k_{m-1}=\{m-1\}$。另一方面，我们也知道1的m次方根（即m次单位根，复根）也有m个。

$$\varepsilon_r=e^{2\pi i\frac{r}{m}}=\cos\frac{2\pi r}{m}+i\sin\frac{2\pi r}{m},\ r=0,1,\cdots,m-1.$$

由于当且仅当$a=b+mt$时，$a\equiv b(\bmod m)$，并且

$$a\equiv b(\bmod m)\Longleftrightarrow e^{2\pi i\frac{a}{m}}=e^{2\pi i\frac{b}{m}}.\qquad(5)$$

令　$k_r\longrightarrow e^{2\pi i\frac{r}{m}}$.

下面用$e\left(\frac{r}{m}\right)$表示$e^{2\pi i\frac{r}{m}}$，即$e^{2\pi i\frac{r}{m}}=e\left(\frac{r}{m}\right)$。显然对应关系（5）是模m的剩余类集合R到m次单位根的集合I上的一个一一对应关系。又有

$$a+b\equiv c(\bmod m)\Longleftrightarrow e\left(\frac{a}{m}\right)\cdot e\left(\frac{b}{m}\right)=e\left(\frac{a+b}{m}\right)$$

$$=e\left(\frac{c}{m}\right).$$

也就是说，加群R与乘群I是同构的．因此，可以把抽象的类的加法运算，变成具体的复数的乘法运算，这就是三角和方法来源之一．

所谓三角和（trigonometrical sums）就是形如

$$\sum_x e^{2\pi i f(x)}=\sum_x e\left(f(x)\right)$$

的和，其中f(x)是实函数，x通过预先指定的整数集．

定理3·9 设m是一个正整数，x过模m的完全剩余系，对于给定的整数a，则

$$\sum_x e\left(\frac{ax}{m}\right)=\begin{cases}m, & \text{若 } m\mid a;\\ 0, & \text{若 } m\nmid a.\end{cases}$$

其中$\sum\limits_x$表示展布在x所通过的值上的和数．

证明 当$m\mid a$时，$e\left(\frac{ax}{m}\right)=1$，故$\sum\limits_x e\left(\frac{ax}{m}\right)=m$.

今设$m\nmid a$，则$e\left(\frac{a}{m}\right)\neq 1$，若r是x对模m的最小非负剩余，则

$$e\left(\frac{ax}{m}\right)=e\left(\frac{ar}{m}\right).$$

因为x过模m的完全剩余系，故r过0，1，…，m－1，因此

$$\sum_x e\left(\frac{ax}{m}\right)=\sum_{r=0}^{m-1} e\left(\frac{ar}{m}\right)=\sum_{r=0}^{m-1}\left[e\left(\frac{a}{m}\right)\right]^r$$

$$=\frac{1-\left[e\left(\frac{a}{m}\right)\right]^m}{1-e\left(\frac{a}{m}\right)}=0.$$

例3.7 设整系数多项式$f(x_1, \cdots, x_n)$，m是任一正整数，则

$$f(x_1, \cdots, x_n)\equiv N(\bmod m),\quad 0\leqslant x_i\leqslant m-1 \tag{6}$$

的解答的数目

$$k=\frac{1}{m}\sum_{x_1=0}^{m-1}\cdots\sum_{x_n=0}^{m-1}\sum_{a=0}^{m-1}e\left(\frac{a}{m}[f(x_1, \cdots, x_n)-N]\right) \tag{7}$$

证明 由定理3·9知道

$$\sum_{a=0}^{m-1}e\left(\frac{a}{m}[f(x_1, \cdots, x_n)-N]\right)=\begin{cases}m, & 当m\mid f(x_1, \cdots, x_n)-N时；\\ 0, & 当m\nmid f(x_1, \cdots, x_n)-N时。\end{cases}$$

也就是说，每一组$(x_1, \cdots, x_n)$代入(6)，当它是(6)的一个解时，在(7)右边的和式中出现一个“1”，不是(6)的解时，出现一个“0”。所以(6)的解的数目等于k。

用(7)表示同余式(6)的解数，使同余式问题获得了解析形式。

定理3·10 设α是一个整数，则

$$\int_0^1 e(\alpha x)dx=\begin{cases}1, & 若\alpha=0；\\ 0, & 若\alpha\neq 0.\end{cases}$$

证明 若$\alpha=0$，则$e(\alpha x)=1$。

$$\therefore \quad \int_0^1 e(\alpha x)dx = 1.$$

若$\alpha \neq 0$，则

$$\int_0^1 e(\alpha x)dx = \int_0^1 \cos(2\pi\alpha x)dx + i\int_0^1 \sin(2\pi\alpha x)dx$$

$$= \left[\frac{\sin 2\pi\alpha x}{2\pi\alpha}\right]_0^1 + i\left[\frac{-\cos 2\pi\alpha x}{2\pi\alpha}\right]_0^1 = 0 + 0i = 0.$$

例3.8 证明，不定方程

$$f(x_1, \cdots, x_n) = N, \quad a_\nu \leqslant x_\nu \leqslant b_\nu \tag{8}$$

的整数解的数目

$$k = \sum_{a_1 \leqslant x_1 \leqslant b_1} \cdots \sum_{a_n \leqslant x_n \leqslant b_n} \int_0^1 e\Big([f(x_1, \cdots, x_n) - N]\, y\Big)dy \tag{9}$$

证明 由定理3.10知道

$$\int_0^1 e\Big([f(x_1, \cdots, x_n) - N]\, y\Big)dy = \begin{cases} 1, & 当 f(x_1, \cdots, x_n) - N = 0, \\ 0, & 当 f(x_1, \cdots, x_n) - N \neq 0. \end{cases}$$

所以(8)的解数等于k。

这使不定方程，得到了解析形式。

例3·9 要证费马大定理，只须证，当$k \geqslant 3$时，

$$\sum_{z=1}^{N}\sum_{y=1}^{N}\sum_{x=1}^{N}\int_0^1 e\Big((x^k + y^k - z^k)\alpha\Big)d\alpha = 0 \tag{10}$$

$$\because \quad \sum_{z=1}^{N}\sum_{y=1}^{N}\sum_{x=1}^{N} e\Big((x^k + y^k - z^k)\alpha\Big) = [e(1^k\alpha) + e(2^k\alpha) +$$

$\cdots+e(N^k\alpha)]\,[e(1^k\alpha)+\cdots+e(N^k\alpha)]\,[e(-1^k\alpha)$
$\cdots+e(-N^k\alpha))$

$$=\left(\sum_{x=1}^{N} e(x^k\alpha)\right)^2\left(\sum_{x=1}^{N} e(-x^k\alpha)\right),$$

∴只须证，$\int_0^1\left(\sum_{x=1}^{N} e(x^k\alpha)\right)^2\left(\sum_{x=1}^{N} e(-x^k\alpha)\right)d\alpha$

$$=0. \tag{11}$$

例3.10 要证哥德巴赫猜想，只需证，当N充分大时，$p_1+p_2-2N=0$，p_1，p_2有素数解，即

$$\sum_{p_2=2N-p_1}\ \sum_{p<2N}\int_0^1 e\Big((p_1+p_2-2N)\alpha\Big)d\alpha$$

$$=\int_0^1\Big(\sum_{p_1<2N} e(p\alpha)\Big)^2 e(-2N\alpha)d\alpha>0. \tag{12}$$

实质上，例3·9，3·10并未给我们解答此二问题以任何的帮助。

定理3·11 设α是任一实数，q与q'是整数，且$q'>q$，则

$$\left|\sum_{x=q+1}^{q'} e(\alpha x)\right|\leqslant\min\left(q'-q,\ \frac{1}{h\langle\alpha\rangle}\right).$$

其中$\min\left(q'-q,\ \frac{1}{h\langle\alpha\rangle}\right)$表示$q'-q$及$\frac{1}{h\langle\alpha\rangle}$中较小的一个数，$\langle\alpha\rangle=\min(\{\alpha\},\ 1-\{\alpha\})$，当$\langle\alpha\rangle\leqslant\frac{1}{2}$时，$h\geqslant2$；但当$\langle\alpha\rangle\leqslant\frac{1}{6}$时，$h\geqslant3$.

证明 令$s=\sum_{x=q+1}^{q'} e(\alpha x)$，因为

$$|e(\alpha x)| = (\cos^2 2\pi\alpha x+\sin^2 2\pi\alpha x)^{\frac{1}{2}} = 1,$$

$$\therefore\quad |s|\leqslant \sum_{x=q+1}^{q'} |e(\alpha x)| = \sum_{x=q+1}^{q'} 1 = q'-q.$$

若α不是整数时，则$e(\alpha)\neq 1$，因此

$$s=e\Big((q+1)\alpha\Big)\Big[\sum_{x=0}^{q'-q-1} e(\alpha x)\Big]$$

$$=e\Big((q+1)\alpha\Big)\frac{1-e\Big((q'-q)\alpha\Big)}{1-e(\alpha)}.$$

$$\because\quad \Big|e\Big((q+1)\alpha\Big)\Big| = 1,$$

$$\Big|e\Big(\frac{\alpha}{2}\Big)-e\Big(-\frac{\alpha}{2}\Big)\Big| = \Big|e^{\pi i\alpha}-e^{-\pi i\alpha}\Big|$$

$$=\Big|\frac{e^{2\pi i\alpha}-1}{e^{\pi i\alpha}}\Big|$$

$$=\Big|1-e(\alpha)\Big|$$

$$\therefore\quad |s| = \left|\frac{1-e\Big((q'-q)\alpha\Big)}{1-e(\alpha)}\right|$$

$$=\frac{\sqrt{(1-\cos 2\pi(q'-q)\alpha)^2+(-\sin 2\pi(q'-q)\alpha)^2}}{\Big|e\Big(\frac{\alpha}{2}\Big)-e\Big(-\frac{\alpha}{2}\Big)\Big|}$$

$$=\frac{\sqrt{2-2\cos 2\pi(q'-q)\alpha}}{|2\sin\pi\alpha|}\leqslant\frac{2}{2|\sin\pi\alpha|}$$

$$=\frac{1}{|\sin\pi\alpha|}.$$

但$|\sin\pi\alpha| = |\sin(\pi[\alpha] + \pi\{\alpha\})| = \sin\pi\{\alpha\}$

$= \sin\pi(1 - \{\alpha\}) = \sin\pi\langle\alpha\rangle$。当$0 < x \leqslant \frac{1}{2}$时$\frac{\sin\pi x}{x}$是递降函数。事实上，令$y = \pi x$，则$\frac{\sin\pi x}{x} = \pi\frac{\sin y}{y}$，

而$\left(\frac{\sin y}{y}\right)' = \frac{y\cos y - \sin y}{y^2} = \frac{1}{y^2}\cos y(y - \operatorname{tg} y) < 0$

$\left(0 < y < \frac{\pi}{2}\right)$。又因$0 < \langle\alpha\rangle \leqslant \frac{1}{2}$，故

$$\frac{\sin\pi\langle\alpha\rangle}{\langle\alpha\rangle} \geqslant \frac{\sin\frac{\pi}{2}}{\frac{1}{2}} = 2 \Longrightarrow \frac{1}{\sin\pi\langle\alpha\rangle}$$

$$\leqslant \frac{1}{2\langle\alpha\rangle},$$

此时有$h \geqslant 2$的h适合

$$|s| \leqslant \frac{1}{h\langle\alpha\rangle}.$$

又当$\langle\alpha\rangle \leqslant \frac{1}{6}$时，

$$\frac{\sin\pi\langle\alpha\rangle}{\langle\alpha\rangle} \geqslant \frac{\sin\frac{\pi}{6}}{\frac{1}{6}} = 3 \Longrightarrow \frac{1}{\sin\pi\langle\alpha\rangle} \leqslant \frac{1}{3\langle\alpha\rangle},$$

此时有$h \geqslant 3$的h适合

$$|s| \leqslant \frac{1}{h\langle\alpha\rangle}.$$

$$\therefore \quad |s| \leqslant \min\left(q' - q, \frac{1}{h\langle\alpha\rangle}\right).$$

定理3.12 若m是大于1的整数，$q(a)$，$q'(a)$是定义在整数$a = 1, 2, \cdots, m - 1$上的整值函数，且$q'(a) >$

$q(a)$。则

$$\sum_{a=1}^{m-1}\left|\sum_{x=q(a)+1}^{q'(a)} e\left(\frac{ax}{m}\right)\right| < m\ln m - \delta$$

其中 $\delta \geqslant \begin{cases} \frac{m}{3}\ln\left(2\left[\frac{m}{6}\right]+1\right)，当m>1时； \\ \frac{m}{2}，当m\geqslant 12时； \\ m，当m\geqslant 60时。\end{cases}$

此定理包含了定理3.11中取 $\alpha=\frac{a}{m}$，$q'=q(a)$，$q=q(a)$时，和式 $\sum\limits_{\alpha=1}^{m-1}$ 的上界。

证明 由 $0<a<m$ 知，$\left\langle\frac{a}{m}\right\rangle\neq 0$，并且

$$\left\langle\frac{a}{m}\right\rangle=\begin{cases}\frac{a}{m}，当 0<a\leqslant\frac{m}{2}时； \\ \frac{m-a}{m}，当\frac{m}{2}<a<m时。\end{cases} \tag{α}$$

由定理3.11得

$$\sum_{a=1}^{m-1}\left|\sum_{x=q(a)+1}^{q'(a)} e\left(\frac{ax}{m}\right)\right| \leqslant \sum_{a=1}^{m-1}\frac{1}{h<\left\langle\frac{a}{m}\right\rangle}$$

令 $\sum\limits_{a=1}^{m-1}\dfrac{1}{h\left\langle\frac{a}{m}\right\rangle}=T_m$，则当m是奇数时，由($\alpha$)式得

$$T_m=\sum_{a=1}^{\left[\frac{m}{2}\right]}\frac{2}{h\left\langle\frac{a}{m}\right\rangle}=\sum_{a=1}^{\left[\frac{m}{2}\right]}\frac{2}{h\frac{a}{m}}$$

$$\leqslant \frac{2m}{3} \sum_{0<a\leqslant \frac{m}{6}} \frac{1}{a} + m \sum_{\frac{m}{6}<a<\frac{m}{2}} \frac{1}{a}$$

$$= m \sum_{0<a<\frac{m}{2}} \frac{1}{a} - \frac{1}{3} m \sum_{0<a\leqslant\frac{m}{6}} \frac{1}{a}. \qquad (\beta)$$

由公式：$l_n(1+x)=x-\frac{x^2}{2}+\frac{x^3}{3}-\cdots(|x|<1)$，得

$$\ln\frac{2a+1}{2a-1}=l_n\frac{1+\frac{1}{2a}}{1-\frac{1}{2a}}=\ln\left(1+\frac{1}{2a}\right)-\ln\left(1-\frac{1}{2a}\right)$$

$$=\frac{1}{2a}-\frac{1}{2}\left(\frac{1}{2a}\right)^2+\frac{1}{3}\left(\frac{1}{2a}\right)^3-\cdots$$

$$-\left[-\frac{1}{2a}-\frac{1}{2}\left(\frac{1}{2a}\right)^2-\frac{1}{3}\left(\frac{1}{2a}\right)^3-\cdots\right]$$

$$=\frac{1}{a}+\frac{2}{3}\left(\frac{1}{2a}\right)^3+\frac{2}{5}\left(\frac{1}{2a}\right)^5+\cdots$$

$$>\frac{1}{a} \qquad (\gamma)$$

代入(β)得

$$T_m<m\sum_{0<a<\frac{m}{2}}\ln\frac{2a+1}{2a-1}-\frac{m}{3}\sum_{0<a\leqslant\frac{m}{6}}\ln\frac{2a+1}{2a-1}$$

$$=m\ln m-\frac{m}{3}\ln\left(2\left[\frac{m}{6}\right]+1\right). \qquad (\delta)$$

事实上，(δ)里的

$$\sum_{0<a<\frac{m}{2}}\ln\frac{2a+1}{2a-1}=\ln\frac{m}{m-2}+\ln\frac{m-2}{m-4}+\cdots$$

$$+\ln\frac{3}{1}=\ln m;$$

$$\sum_{0<a\leqslant\frac{m}{6}}\ln\frac{2a+1}{2a-1}=\ln\frac{2\left[\frac{m}{6}\right]+1}{2\left[\frac{m}{6}\right]-1}$$

$$+\ln\frac{2\left[\frac{m}{6}\right]-1}{2\left[\frac{m}{6}\right]-3}+\cdots+\ln\frac{3}{1}$$

$$=\ln\left(2\left[\frac{m}{6}\right]+1\right).$$

$$\therefore\quad \delta=\frac{m}{3}\ln\left(2\left[\frac{m}{6}\right]+1\right)(m>1).$$

当$m=13$时，$\delta=\frac{m}{3}\ln 5=\frac{m}{3}\times 1.60944>\frac{m}{2}$，

当$m=61$时，$\delta=\frac{m}{3}\ln 21=\frac{m}{3}\times 3.04452>m$。

当m是偶数时，

$$Tm=\sum_{a=1}^{m-1}\frac{1}{h\langle\frac{a}{m}\rangle}=m\sum_{0<a\leqslant\frac{m}{2}}\frac{1}{ha}$$

$$+m\sum_{\frac{m}{2}<a<m}\frac{1}{h(m-a)},$$

后一项用a代$m-a$得$m\sum_{0<a\leqslant\frac{m}{2}}\frac{1}{ha}$（$\because\frac{m}{2}<a<m$

$\Leftrightarrow\frac{m}{2}>m-a>0$）。

$$\therefore\quad T_m = m\sum_{0<a\leqslant\frac{m}{2}}\frac{1}{ha} + m\sum_{0<a<\frac{m}{2}}\frac{1}{ha}$$

$$= m\sum_{0<a\leqslant\frac{m}{6}}\frac{1}{3a} + m\sum_{\frac{m}{6}<a\leqslant\frac{m}{2}}\frac{1}{2a}$$

$$+ m\sum_{0<a\leqslant\frac{m}{6}}\frac{1}{3a} + m\sum_{\frac{m}{6}<a<\frac{m}{2}}\frac{1}{2a}$$

$$= \frac{2}{3}m\sum_{0<a\leqslant\frac{m}{6}}\frac{1}{a} + m\sum_{\frac{m}{6}<a<\frac{m}{2}}\frac{1}{a} + m\cdot\frac{1}{2\frac{m}{2}}$$

$$= m\sum_{0<a<\frac{m}{2}}\frac{1}{a} - \frac{1}{3}m\sum_{0<a\leqslant\frac{m}{6}}\frac{1}{a} + 1$$

$$< m\sum_{0<a<\frac{m}{2}}\ln\frac{2a+1}{2a-1} - \frac{1}{3}m\sum_{0<a\leqslant\frac{m}{6}}\ln\frac{2a+1}{2a-1}$$

$$+ 1 = m\ln(m-1) - \frac{1}{3}m\ln\left(2\left[\frac{m}{6}\right]+1\right)$$

$$+ 1 = m\ln m + m\ln\left(1-\frac{1}{m}\right)$$

$$-\frac{1}{3}m\ln\left(2\left[\frac{m}{6}\right]+1\right) + 1 < m\ln m$$

$$-\frac{1}{3}m\ln\left(2\left[\frac{m}{6}\right]+1\right).$$

即$\delta = \frac{m}{3}\ln\left(2\left[\frac{m}{6}\right]+1\right)$与m为奇数的情况，同样地讨论，可得所要的结论。故定理得证。

习　题

1．找出整数被37、101整除的一种判别法。

2．用弃九法验算下列计算是否正确？

(i)　$4568\times7391=30746529$；

(ii)　$16\times937\times1559=23373528$。

3．用检验因数法，求1535625的标准分解式。

4．问0，2^1，2^2，…，2^{10}是否构成模11的完全剩余系？

5．证明，若a是奇数，则

$$a^{2^n}\equiv1\pmod{2^{n+2}},\quad(n\geqslant1).$$

6．证明，

$$x=u+p^{s-t}v\ (t\leqslant s)$$

是模p^s的一个完全剩余系，其中u，v分别过模p^{s-t}和p^t的完全剩余系。

7．若m_1，m_2，…，m_k是k个两两互素的正整数，x_1，x_2，…，x_k分别过模m_1，m_2，…，m_k的完全剩余系，则

$$M_1x_1+M_2x_2+\cdots+M_kx_k$$

过模$m=m_1m_2\cdots m_k$的完全剩余系，其中$m=m_iM_i(i=1,\ 2,\ \cdots,\ k)$。

8．(i)　证明，整数数列

$$-H,\ \cdots,\ -1,\ 0,\ 1,\ \cdots,\ H\ \left(H=\frac{3^{n+1}-1}{3-1}\right)$$

中的每一个数，有且只有一种方法，表示成

$$3^nx_n+3^{n-1}x_{n-1}+\cdots+3x_1+x_0 \tag{a}$$

的形状，其中$x_i=-1$，0，或1．反之，(a)中每一个数都大于或等于$-H$，并且小于或等于H。

(ii)　说明应用$n+1$个特制的砝码，在天秤上可以量出1到H中的任何一个斤数。

9．若m_1，…，m_k是k个两两互素的正整数，x_1，…，x_k分别过模m_1，…，m_k的完全剩余系。则

$$x_1+m_1x_2+m_1m_2x_3+\cdots+m_1\cdots m_{k-1}x_k \qquad (a)$$

过模$m_1m_2\cdots m_k$的完全剩余系。

10 若m是大于1的整数，$(a, m)=1$，ξ过模m的互素剩余系，则

$$\sum_{\xi}\left\{\frac{a\xi}{m}\right\}=\frac{1}{2}\varphi(m).$$

其中$\sum\limits_{\xi}$表示展布在ξ所通过的一切值上的和式。

11. 若$m_1, m_2, \cdots, m_k$是k个两两互素的正整数，$\xi_1, \xi_2, \cdots, \xi_k$分别过模$m_1, m_2, \cdots, m_k$的互素剩余系，$m=m_iM_i(i=1, \cdots, k)$，则

$$M_1\xi_1+M_2\xi_2+\cdots+M_k\xi_k$$

过模$m=m_1m_2\cdots m_k$的互素剩余系。

12. 求$(7222^{37}+3)^{18}$被63除的余数。

13. (i) 不用定理3.7系2，证明，若p是素数，$h_1h_2, \cdots, h_t$是任意整数，则

$$(h_1+h_2+\cdots+h_t)^p\equiv h_1^p+h_2^p+\cdots+h_t^p \pmod{p}.$$

(ii) 由(i)证明定理3·7系2.

(iii) 证明欧拉定理。

第四章　同　余　式

解代数方程是初等代数的主要内容之一，本章所要讨论的解同余式的问题，与解代数方程十分类似，例如，我们问当x与什么数同余时，能使

$$x^6+x+1\equiv 0\ (\bmod\ 7)$$

成立？这就是解同余式的问题。由验算知道 $x\equiv 2\ (\bmod\ 7)$ 是它的一个解。本章主要介绍一次同余式，一次同余式组及高次同余式，并在一次同余式组一节里介绍举世闻名的孙子定理（有些外文书中称为中国剩余定理），从而说明中国古代数学家在这方面的光辉成就。

第一节　一元一次同余式

定义 4·1　给定一个正整数m，整系数多项式 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$，我们把

$$f(x)\equiv 0\ (\bmod\ m) \tag{1}$$

叫做模 m 的同余式（congruence of modulus m），若 $a_n\not\equiv 0\ (\bmod\ m)$，则称n是（1）的次数（degree）。如果 $f(a)\equiv 0\ (\bmod\ m)$，由同余的性质 4°知道 $a'\equiv a\ (\bmod\ m)$ 时，$f(a')\equiv 0\ (\bmod\ m)$。即模m的剩余类{a}中任一整数都满足（1）。所以称 $x\equiv a\ (\bmod\ m)$ 是（1）的一个解（solution）。

当n＝1时，同余式

$$ax\equiv b\ (\bmod\ m),\quad a\not\equiv 0\ (\bmod\ m), \tag{2}$$

称为一元一次同余式。

由同余的定义知道，（2）有解的充要条件是：存在整数

x，y 3 $ax-my=b$。这不定方程有解的充要条件是：$(a, m)|b$。

如果$(a, m)=d$，$m_1=\frac{m}{d}$，$a_1=\frac{a}{d}$，$b_1=\frac{b}{d}$为整数，且$x\equiv x_0 \pmod m$是(2)的一个解，那末存在y_0使得$ax_0-my_0=b$（即$a_1x_0-m_1y_0=b_1$）这样的(x_0, y_0)是

$$ax-my=b \tag{2'}$$

的一个整数解。由定理2·1知道(2′)的一切整数解是：

$x=x_0+m_1t$，$y=y_0+a_1t$，$t=0, \pm1, \pm2, \cdots$ 上面第一式对于模m来说，可以写成

$$x\equiv x_0+km_1 \pmod m,\quad k=0, 1, \cdots, d-1 \tag{3}$$

它表示关于模m的d个不同的类，故(2)有形如(3)的d个解。这就证明了

定理 4·1 一次同余式(2)有解的充要条件是：$(a, m)|b$。若(2)有解时，则其解数是：$d=(a, m)$。

例4·1 解同余式

$$58x\equiv87 \pmod{47} \tag{a}$$

解 先将诸系数用它们关于模47的最小正剩余来代替，得

$$11x\equiv40 \pmod{47} \tag{a'}$$

因为$(11, 47)=1$，所以(a)有且只有一个解。先求同余式$11x'\equiv1 \pmod{47}$的解。由第二章知道，可用大衍求一术求$11x'-47y'=1$的解：

$$11\times2=47\times0+22,$$

$$11\times5=47\times1+8,$$

$$11\times5\times3=47\times3+24,$$

$$11\times17=47\times4-1,$$

$$\therefore\quad 11\times(-17)=47\times(-4)+1.$$

所以$x'=-17$。因而$x\equiv(-17)\times40\equiv25\pmod{47}$是(a)的唯一解。

另一种解法，用辗转相除法，先把$\frac{47}{11}$化成连分数

$$\begin{aligned}47:11&=4\\11:3&=3\\3:2&=1\\2:1&=2\end{aligned}\quad\therefore\ \frac{47}{11}=[4,\ 3,\ 1,\ 2]$$

则$-y'=(-1)^4\{3,\ 1\}=4\Longrightarrow y'=-4$，$x'=(-1)^3\{4,\ 3,\ 1\}=-17$是不定方程$11x'-47y'=1$的解。即

$$x\equiv25\pmod{47}$$

是(a)的解。

由定理4·1知道，要求同余式(2)的$d=(a,\ m)$个解时，可先求下列同余式的解

$$a_1x\equiv b_1\pmod{m_1}$$

其中$a=a_1d$，$b=b_1d$，$m=m_1d$，$(a_1,\ m_1)=1$。次按(3)给出(2)的d个解。

例如，求$9x\equiv6\pmod{15}$的解。先求$3x\equiv2\pmod5$的解，$x\equiv4\pmod5$。次求出$x\equiv4,\ 9,\ 14\pmod{15}$是$9x\equiv6\pmod{15}$的三个解。

定理4·2 设m是正整数，$(a,\ m)=1$，证明

$$x\equiv b\,a^{\varphi(m)-1}\pmod m$$

是(2)的唯一解。

证明 由定理4·1知道，当$(a,\ m)=1$时，(2)有唯一的解。应用欧拉定理，易得

$$a\times b\,a^{\varphi(m)-1}=b\cdot a^{\varphi(m)}\equiv b\pmod m.$$

所以$x\equiv ba^{\varphi(m)-1}$是(2)的唯一解。

系 设p是素数，$0<a<p$，证明

$$x \equiv b(-1)^{a-1}\frac{(p-1)(p-2)\cdots(p-a+1)}{a!}(\bmod\ p) \qquad (\alpha)$$

是(2)的唯一解。

证明 因为a个连续整数之积被a!所整除，又p是大于a的素数，$(p, a)=1$，所以(α)的右边是整数，且(2)有唯一解。令

$$a\,b(-1)^{a-1}\frac{(p-1)(p-2)\cdots(p-a+1)}{a!}=k$$

$$\Longrightarrow b(-1)^{a-1}(p-1)(p-2)\cdots(p-a+1)=k(a-1)!$$

上式左边$\equiv b(-1)^{2(a-1)}(a-1)!(\bmod\ p)$。

$$\therefore\quad b(-1)^{2(a-1)}(a-1)!\equiv k(a-1)!\ (\bmod\ p)$$

即 $$k\equiv b\ (\bmod\ p)。$$

所以(α)是(2)的唯一解。

定理4·2及系给出了解一元一次同余式的公式。系的计算量较少，但仅适用于素数模的情况。

例4·2 求下列同余式的解：

(i) $3x\equiv 7\ (\bmod\ 13)$；

(ii) $11x\equiv 15\ (\bmod\ 24)$。

解 (i) $3x\equiv 7\ (\bmod\ 13)$的唯一解是：

$$x\equiv 7\times(-1)^2\frac{(13-1)(13-2)}{3!}\equiv 11(\bmod\ 13)。$$

(ii) 因为$(11, 24)=1$，所以该同余式有唯一解

$$x\equiv 15\times 11^{\varphi(24)-1}(\bmod\ 24)。$$

而$\varphi(24)=8$，$11^2=121\equiv 1(\bmod 24) \Longrightarrow 11^6\equiv 1(\bmod\ 24)$
$\Longrightarrow 11^7\equiv 11(\bmod\ 24)$

$$\therefore\quad x\equiv 15\times 11^7\equiv 15\times 11\equiv -3(\bmod\ 24)。$$

第二节　一元一次同余式组

公元前后《孙子算经》中记载有："今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何？""答曰二十三"，这就是求一元一次同余式组

$$\begin{cases} x \equiv 2 \pmod 3, \\ x \equiv 3 \pmod 5, \\ x \equiv 2 \pmod 7. \end{cases} \tag{4}$$

的解。$x = 23$是(4)的三个同余式的公共解。

定义 4·2　一个变数x的同余式组

$$\begin{cases} a_1x + b_1 \equiv 0 \pmod{m_1}, \\ a_2x + b_2 \equiv 0 \pmod{m_2}, \\ \cdots \quad \cdots \quad \cdots \quad , \\ a_Sx + b_S \equiv 0 \pmod{m_S}. \end{cases} \tag{5}$$

称为一元一次同余式组（linear congruences of one unknown）。$x \equiv c \pmod{[m_1, \cdots, m_s]}$满足(5)中任一同余式时，称为(5)的一个解。

例如，$x \equiv 23 \pmod{105}$是(4)的一个解。关于解一般同余式组

$$\begin{cases} x \equiv a \pmod 3, \\ x \equiv b \pmod 5, \\ x \equiv c \pmod 7. \end{cases} \tag{6}$$

则有

$$x \equiv 70a + 21b + 15c \pmod{105}$$

是(6)的一个解。

在明朝程大位的《算法统宗》(1593)里，用一首歌诀来表示(6)的解：

三人同行七十稀，

五树梅花廿一枝，

七子团圆正半月，

除百零五便得知。

这些足以说明，解同余式组的问题，我国古代已有了光辉的成就。下面将介绍驰名中外的孙子定理，有的外文书中称它为中国剩余定理（Chinese Remainder Theorem）。

定理 4·3 （孙子定理）若$k\geqslant 2$，且m_1，…，m_k是两两互素的k个正整数，令

$M=m_1\cdots m_k=m_1M_1=\cdots=m_kM_k$，

那末满足同余组

$$\begin{cases} x\equiv b_1\ (\bmod m_1), \\ \cdots\quad \cdots\quad \cdots, \\ x\equiv b_k\ (\bmod m_k) \end{cases} \tag{7}$$

的整数解是

$$x\equiv b_1M_1'M_1+\cdots+b_kM_k'M_k\ (\bmod M) \tag{8}$$

这里M_i'是满足同余式

$$M_i'M_i\equiv 1\ (\bmod m_i),\ (i=1,\ \cdots,\ k) \tag{9}$$

的整数解，并且(7)的解是唯一的。

证明 因为m_1，…，m_k两两互素，且$M_i=\dfrac{M}{m_i}$，所以

$(M_1,\ m_1)=\cdots=(M_k,\ m_k)=1$。

由定理1·12知道，存在二整数M_i'，n_i使得$M_i'M_i+n_im_i=1$，亦即存在一个整数M_i'使得

$$M_i'M_i\equiv 1\ (\bmod m_i)\ (i=1,\ \cdots,\ k). \tag{9}$$

另一方面，当 $i \neq j$ 时，$m_i \mid M_j$

$$\therefore \quad b_j M_j' M_j \equiv 0 \pmod{m_i} \tag{10}$$

由(a)及(10)立即得到

$$b_1 M_1' M_1 + \cdots + b_k M_k' M_k \equiv b_i M_i' M_i \equiv b_i \pmod{m_i} \tag{11}$$

其中 $i=1, \cdots, k$。所以(8)是(7)的一个解

最后证明(7)的解是唯一的。如果y亦是(7)的解。那末

$$x \equiv b_i \equiv y \pmod{m_i} \quad (i=1, \cdots, k)$$

即 $m_i \mid (x-y)(i=1, \cdots, k)$。由于 $i \neq j$ 时 $(m_i, m_j)=1$，由整除的性质11°，得

$$m_1 \cdots m_k \mid (x-y)$$

$$\therefore \quad x \equiv y \pmod{M}.$$

这就证明了，(7)的解是唯一的。

例 4·3 （韩信点兵问题）有兵一队，若列成五行纵队，则末行一人；列成六行纵队，则末行五人；列成七行纵队，则末行四人；列成十一行纵队，则末行十人，求兵数。

解 设 x是所求的兵数，则依题意，得

$$\begin{cases} x \equiv 1 \pmod{5}, \\ x \equiv 5 \pmod{6}, \\ x \equiv 4 \pmod{7}, \\ x \equiv 10 \pmod{11}. \end{cases}$$

因为 5，6，7，11两两互素，由定理 4·3 知，

$M = 5 \times 6 \times 7 \times 11 = 2310$，$M_1 = \frac{2310}{5} = 462$，$M_2 = \frac{2310}{6} = 385$，$M_3 = \frac{2310}{7} = 330$，$M_4 = \frac{2310}{11} = 210$

$M_1' M_1 \equiv M_1' \cdot 2 \equiv 1 \pmod{5} \Longrightarrow M_1' \equiv 3 \pmod{5}$，同 理

求得，$M_2' \equiv 5 \pmod{6}$，$M_3' \equiv 4 \pmod{7}$，$M_4' \equiv 1 \pmod{11}$.

$$\therefore \quad x \equiv 3\times 462 + 5\times 385 + 4\times 330 + 10\times 210$$
$$= 6731 \equiv 2111 \pmod{2310}$$

所以韩信的兵数有$x = 2111 + k\times 2310 (k = 0, 1, \cdots)$

是否同余式组(5)都有解呢？首先必须(5)中每一个同余式都有解，其次，再考虑它们是否有公共解。所以首先假设(5)的每一个同余式都有解，用(7)表示它们的解。进而研究(7)在什么条件下有解(有公共解)。

定理 4·4 如果同余式组(7)有解，那末它关于模$M = [m_1, \cdots, m_k]$有唯一解。

证明 若α与β是(7)的两个解，则

$$\alpha \equiv b_i \pmod{m_i},\ \beta \equiv b_i \pmod{m_i} (i = 1, \cdots, k).$$

$$\therefore \quad \alpha \equiv \beta \pmod{m_i} \Longrightarrow m_i \mid \alpha - \beta (i = 1, \cdots, k)$$
$$\Longrightarrow [m_1, \cdots, m_k] \mid \alpha - \beta \Longrightarrow$$

$\alpha \equiv \beta (\bmod [m_1, \cdots, m_k])$.

定理 4·5 若$m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$是模m的标准分解式，则同余式

$$x \equiv a \pmod{m} \tag{12}$$

与同余式组

$$\begin{cases} x \equiv a (\bmod p_1^{\alpha_1}), \\ \cdots \quad \cdots \quad \cdots, \\ x \equiv a (\bmod p_k^{\alpha_k}). \end{cases} \tag{13}$$

同解。

证明 设$x \equiv b \pmod{m}$是(12)的一个解，即

$b \equiv a \pmod{m} \Longrightarrow m \mid (b - a) \Longrightarrow p_i^{\alpha_i} \mid (b - a) (i = 1,$

$\cdots, k) \Longrightarrow b \equiv a(\bmod p_i^{\alpha_i})(i=1, \cdots, k)$。

反之，若b是同余式组(13)的一个解，即

$b \equiv a(\bmod p_i^{\alpha_i})(i=1, \cdots, k) \Longrightarrow p_i^{\alpha_i} \mid (b-a)\ (i=1,$

$\cdots, k) \Longrightarrow m \mid (b-a) \Longrightarrow b \equiv a(\bmod m)$。

系　同余组(7)和同余式组

$$\left\{\begin{array}{l} x \equiv b_1(\bmod p_{11}^{\alpha_{11}}), \\ \cdots \quad \cdots \quad \cdots, \\ x \equiv b_1(\bmod p_{1s}^{\alpha_{1s}}); \\ x \equiv b_2(\bmod p_{21}^{\alpha_{21}}), \\ \cdots \quad \cdots \quad \cdots, \\ x \equiv b_2(\bmod p_{2t}^{\alpha_{2t}}); \\ \cdots \quad \cdots \quad \cdots, \\ x \equiv b_k(\bmod p_{ku}^{\alpha_{ku}}). \end{array}\right. \tag{14}$$

同解，其中

$$m_1 = p_{11}^{\alpha_{11}} \cdots p_{1s}^{\alpha_{1s}},\quad m_2 = p_{21}^{\alpha_{21}} \cdots p_{2t}^{\alpha_{2t}},\quad \cdots,\quad m_k = p_{k1}^{\alpha_{k1}} \cdots p_{ku}^{\alpha_{ku}}.$$

下面证明，同余式组(7)解的存在性定理。

定理 4·6　同余式组(7)有解的充要条件是：

$$b_i \equiv b_j(\bmod (m_i, m_j))(i \neq j;\ i, j=1, \cdots, k) \tag{15}$$

证明　设(7)有解α，则当$i \neq j$时

$\alpha \equiv b_i(\bmod m_i)$，$\alpha \equiv b_j(\bmod m_j) \Longrightarrow m_i \mid (\alpha - b_i)$且

$m_j \mid (\alpha - b_j)$

又因$(m_i, m_j) \mid m_i$，$(m_i, m_j) \mid m_j$

$\therefore \quad (m_i, m_j) | (\alpha - b_i), (m_i, m_j) | (\alpha - b_j)$

即 $\qquad \alpha \equiv b_i \equiv b_z (\bmod (m_i, m_j))$.

反之，若$b_1, b_2, \cdots b_k$满足条件(15)，由于(7)和(14)同解，为了方便，在(14)中，令

$$p_{11}^{\alpha_{11}} = n_{11}, \cdots, p_{1s}^{\alpha_{1s}} = n_{1s}; \ p_{21}^{\alpha_{21}} = n_{21}, \cdots, p_{2t}^{\alpha_{2t}} = n_{2t}; \cdots; \ p_{k1}^{\alpha_{k1}} = n_{k1}, \cdots, p_{ku}^{\alpha_{ku}} = n_{ku}.$$

由条件(15)可以推得

$$b_i \equiv b_j (\bmod (n_{i_u}, n_{j_v})),$$

因为$(n_{i_u}, n_{j_v}) | (m_i, m_j)$.

可能有两种情况：或者n_{i_u}和n_{j_v}是同一素数p的乘幂；或者是不同素数的乘幂.

Ⅰ. 若$n_{i_u} = p^\alpha$, $n_{j_v} = p^\beta$，可设 $\alpha \geqslant \beta$，则(14)中的同余式组

$$\begin{cases} x \equiv b_i (\bmod n_{i_u}), \\ x \equiv b_j (\bmod n_{j_v}); \end{cases} \quad 即 \begin{cases} x \equiv b_i (\bmod p^\alpha), \\ x \equiv b_j (\bmod p^\beta). \end{cases} \tag{16}$$

如果c是(16)第一式的一个解，即$c \equiv b_i (\bmod p^\alpha)$，因为$\alpha \geqslant \beta$，所以$c \equiv b_i (\bmod p^\beta)$，但$(p^\alpha, p^\beta) = p^\beta$，因而条件$b_i \equiv b_j (\bmod (n_{i_u}, n_{j_v}))$就是

$$b_i \equiv b_j (\bmod p^\beta).$$

$$\therefore \quad c \equiv b_j (\bmod p^\beta).$$

因此c也是(16)第二式的解. 由于(16)是(14)中任意两具有上述条件的同余式，(16)第一式的解都是第二式的解，故求(14)中各同余式的公共解时，可以删去(16)的第二式，删去后并不影响(14)与(7)的同解性. 这样继续进行上述方法，使(14)只留下模两两互素的同余式，该同余式组仍与(7)同解，这样把Ⅰ的情况归并于Ⅱ.

Ⅱ. $(n_{i_u}, n_{i_v})=1$，由孙子定理知道(14)有解。

例 4·4 讨论并解答，同余式组

$$\begin{cases} x\equiv 7 \pmod{15}, \\ x\equiv 2 \pmod{35}, \\ x\equiv 16 \pmod{21}. \end{cases} \tag{17}$$

解 ∵ $(15, 35)=5$，而$7\equiv 2 \pmod 5$；

$(15, 21)=3$，而$7\equiv 16 \pmod 3$；

$(35, 21)=7$，而$2\equiv 16 \pmod 7$。

所以(17)有解，它等价（即同解）于

$$\begin{cases} x\equiv 7 \pmod 3, \\ x\equiv 7 \pmod 5, \\ x\equiv 2 \pmod 5, \\ x\equiv 2 \pmod 7, \\ x\equiv 16 \pmod 3, \\ x\equiv 16 \pmod 7. \end{cases}$$

删去"多余"的同余式后，得

$$\begin{cases} x\equiv 7 \pmod 3, \\ x\equiv 7 \pmod 5, \\ x\equiv 2 \pmod 7. \end{cases} \quad 即 \quad \begin{cases} x\equiv 1 \pmod 3, \\ x\equiv 2 \pmod 5, \\ x\equiv 2 \pmod 7. \end{cases}$$

应用孙子定理，求得$M=3\times 5\times 7=105$，$M_1=35$，$M_2=21$，$M_3=15$，$M_1'=2$，$M_2'=1$，$M_3'=1$

∴ $x=1\times 70+2\times 21+2\times 15=142\equiv 37 \pmod{35}$，就是(17)的一个解。

孙子定理是数论中一条重要的定理。从定理4·5知道，要解合数模的一次同余式，转化为解与它同解的模两两互素的一次同余式组，它可以用孙子定理来求解。这种解同余式

的方法具有普遍的意义。为了下一节的需要，最后我们介绍

定理 4·7 若$b_1,\cdots,b_k$分别过模$m_1,\cdots,m_k$的完全剩余系。则孙子定理里的(8)式，过模$M=m_1m_2\cdots m_k$的完全剩余系

证明 令

$$x_0=\sum_{i=1}^{k}M_i'M_ib_i \qquad (8')$$

则当b_i过模m_i $(i=1,\cdots,k)$的完全剩余系时，x_0有$m_1\cdots m_k=M$个值。这M个值关于模M是互不同余的。事实上，若

$$\sum_{i=1}^{k}M_i'M_ib_i'\equiv\sum_{i=1}^{k}M_i'M_ib_i''(\mathrm{mod}\,M),$$

则 $M_i'M_ib_i'\equiv M_i'M_ib_i''(\mathrm{mod}\,m_i)(i=1,\cdots,k)$,

即 $b_i'\equiv b_i''(\mathrm{mod}\ m_i)(i=1,\cdots,k)$

但是b_i'，b_i''是模m_i的同一完全剩余系中的二数，故$b_i'=b_i''$ $(i=1,\cdots,k)$。所以(8′)表示了M个关于模M两两互不同余的数，它形成了模M的一个完全剩余系。

第三节 高次同余式

本节仅初步讨论高次同余式解的数量和解法。主要是把合数模同余式化成素数幂模同余式组，然后讨论它们的解法。

定理 4·8 若$m_1,\cdots,m_k$是k个两两互素的正整数，$m=m_1\cdots m_k$，则同余式

$$f(x)\equiv0(\mathrm{mod}\,m) \qquad (18)$$

与同余式组

$$f(x)\equiv 0(\bmod m_i)(i=1,\ \cdots,\ k) \tag{19}$$

同解。

并且若用T_i表示(19)的第 i 个同余式的解数（关于模 m），T表示(18)的解数（关于模m），则

$$T=T_1T_2\cdots T_k.$$

证明 先证(18)与(19)同解。其证法与定理 4·5 一样。设x_0是适合(18)的整数，则

$$f(x_0)\equiv 0(\bmod m)\Longrightarrow m|f(x_0)\Longrightarrow m_i|f(x_0)\ (i=1,\ \cdots,\ k)$$

$$\Longrightarrow f(x_0)\equiv 0(\bmod m_i)(i=1,\ \cdots,k)$$

反之，若x_0是适合(19)各同余式的整数，则

$$f(x_0)\equiv 0(\bmod m_i)(i=1,\ \cdots,\ k)\Longrightarrow m_i|f(x_0)(i=1,\ \cdots,\ k)$$

$$\Longrightarrow m|f(x_0)\Longrightarrow f(x_0)\equiv 0(\bmod m)$$

所以(18)与(19)同解。

其次，设$f(x)\equiv 0(\bmod m_i)$的T_i个不同的解是

$$x\equiv b_{it_i}(\bmod m_i)(t_i=1,\ \cdots,\ T_i),$$

则(19)的解即下列诸同余式组的解：

$$\begin{cases} x\equiv b_{1t_1}(\bmod m_1),\ (t_1=1,\ \cdots,\ T_1); \\ \cdots\quad \cdots\quad \cdots\quad \cdots; \\ x\equiv b_{kt_k}(\bmod m_k),\ (t_k=1,\ \cdots,\ T_k). \end{cases} \tag{20}$$

显然(20)包含$T=T_1\cdots T_k$个同余式组。由孙子定理知道，(20)的每一个同余式组都有关于模m的唯一的解。所以(18)共有T个解。由定理4·7知道这T个解关于模 m是互不同余的。

定理4·5实际是定理4·8的特殊情况.

例 4·5 解同余式

$$f(x)\equiv 0 \pmod{35},\quad f(x)=x^4+2x^3+8x+9 \tag{21}$$

解 由定理48知，(21)与同余式组

$$\begin{cases} f(x)\equiv 0 \pmod 5 \\ f(x)\equiv 0 \pmod 7 \end{cases} \tag{21'}$$

等价（同解）. 容易验证(21′)的第一、二个同余式的解，依次是：

$$x\equiv 1,\ 4 \pmod 5,$$

$$x\equiv 3,\ 5,\ 6 \pmod 7.$$

故同余式(21)有2×3＝6个解，它们是诸同余式组

$$\begin{cases} x\equiv b_1 \pmod 5)(b_1=1,\ 4); \\ x\equiv b_2 \pmod 7)(b_2=3,\ 5,\ 6). \end{cases}$$

的解，由孙子定理得

$$x\equiv 21b_1+15b_2 \pmod{35}$$

以b_1，b_2的值分别代入上式，即得(21)的全部解：

$$x\equiv 31,\ 26,\ 6,\ 24,\ 19,\ 34 \pmod{35}.$$

由算术基本定理知道，任一正整数m可以写成标准分解式

$$m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k},$$

由定理4·8知道，要解同余式(18)，只要解同余组

$$f(x)\equiv 0 \pmod{p_i^{\alpha_i}}\ (i=1,\ 2,\ \cdots,k) \tag{22}$$

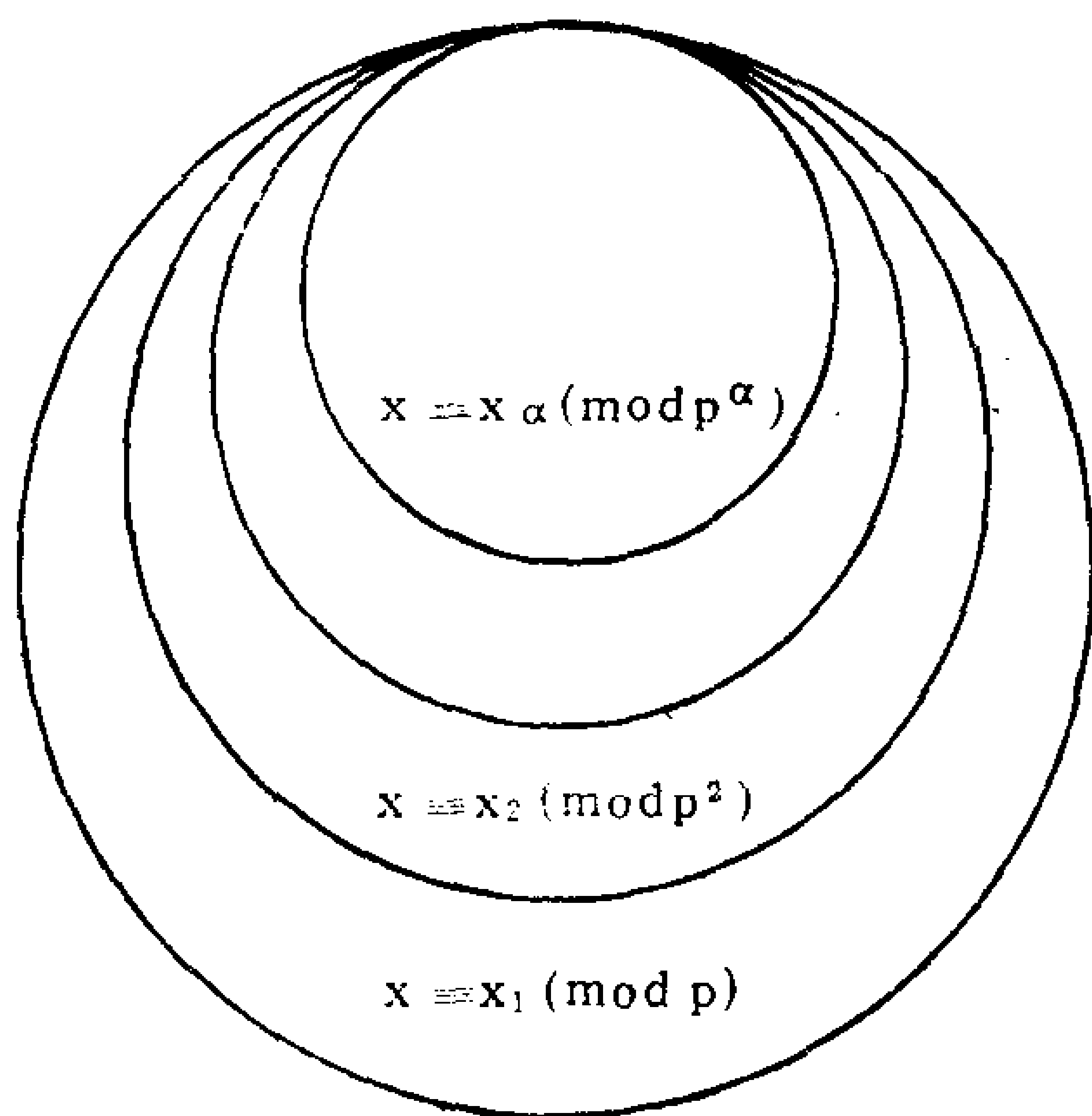
因此下面着重讨论素数幂为模的同余式

$$f(x)\equiv 0 \pmod{p^{\alpha}} \tag{23}$$

的解法. 由同余的性质8°知道，每一个适合(23)的整数，都适合同余式

$$f(x)\equiv 0 \pmod p. \tag{24}$$

因此要求(23)的解，可以从(24)的解中分离出来。通俗地说，也就是从(24)的一个解 $x\equiv x_1 \pmod p$ 中逐步分离出 $x\equiv x_2 \pmod{p^2}$，…，$x\equiv x_\alpha \pmod{p^\alpha}$ 依次是 $f(x)\equiv 0 \pmod p$，$f(x)\equiv 0 \pmod{p^2}$，…，$f(x)\equiv 0 \pmod{p^\alpha}$ 的解。



也就是从模p的一个类 $\{x_1\}_p$ 中找到一个子集，使这个子集是适合(23)的模 p^α 的一个剩余类 $\{x_\alpha\}_{p^\alpha}$(如上图)。

事实上，类 $\{x_1\}_p$ 中包含有 $\{x_1\}_{p^2}$，$\{x_1+p\}_{p^2}$，…，$\{x_1+(p-1)p\}_{p^2}$ 等p个不同的关于模 p^2 的剩余类，其中有一个是 $f(x)\equiv 0 \pmod{p^2}$ 的解。依此类推就可分离出 $x\equiv x_p \pmod{p^\alpha}$ 的剩余类 $\{x_\alpha\}_{p^\alpha}$ 使它是 $f(x)\equiv 0 \pmod{p^\alpha}$ 的一个解。

定理 4·9 设

$$x\equiv x_1 \pmod p$$

即 $x=x_1+pt_1$，$t_1=0$，± 1，± 2，… (25)

是(24)的一个解，并且 $p\nmid f'(x)$($f'(x)$ 是 $f(x)$ 的导数)，则从(25)可刚好给出(23)的一个解(对模 p^α 来说)：

$$x=x_\alpha+p^\alpha_{t\alpha}，\quad t_\alpha=0，\pm 1，\pm 2，\cdots$$

即 $x\equiv x_\alpha \pmod{p^\alpha}$，其中 $x_\alpha\equiv x_1 \pmod p$

证明 我们对于素数p的幂 α，使用数字归纳法证明之。

A) 当 $\alpha=2$ 时，要求同余式 $f(x)\equiv 0 \pmod{p^2}$ 的解由

(25)给出，也就是求满足$f(x_1+pt_1)\equiv 0(\bmod p^2)$的$t_1$，应用泰勒（Tayler）公式，将它的左边展开，即得

$$f(x_1)+pt_1f'(x_1)\equiv 0(\bmod p^2),$$

但是$f(x_1)\equiv 0(\bmod p)$，由同余的性质6°，得到

$$t_1\cdot f'(x_1)\equiv -\frac{f(x_1)}{p}(\bmod p),$$

由于$p\nmid f'(x_1)$，故对模p来说刚好有一解

$$t_1\equiv t_1'(\bmod p)，\text{即}t_1=t_1'+pt_2,$$

代入(25)得

$$x=x_1+p(t_1'+pt_2)=x_2+p^2t_2,$$

其中$x_2=x_1+pt_1'$，显然$x_2\equiv x_1(\bmod p)$，且适合$f(x)\equiv 0(\bmod p^2)$。故$x\equiv x_2(\bmod p^2)$是(25)给出的$f(x)\equiv 0(\bmod p^2)$的唯一解。

B) 设定理对于$\alpha-1$的情形是正确的，即从(25)刚好给出

$$f(x)\equiv 0(\bmod p^{\alpha-1})$$

的一个解：

$$x=x_{\alpha-1}+p^{\alpha-1}t_{\alpha-1},\quad t_{\alpha-1}=0,\ \pm 1,\pm 2,\cdots,$$

$$x_{\alpha-1}\equiv x_1(\bmod p). \tag{a}$$

把它代入(23)，并将左端应用泰勒公式展开，得

$$f(x_{\alpha-1})+p^{\alpha-1}t_{\alpha-1}f'(x_{\alpha-1})\equiv 0(\bmod p^\alpha).$$

但是$f(x_{\alpha-1})\equiv 0(\bmod p^{\alpha-1})$，因此

$$t_{\alpha-1}f'(x_{\alpha-1})\equiv -\frac{f(x_{\alpha-1})}{p^{\alpha-1}}(\bmod p). \tag{b}$$

由$x_{\alpha-1}\equiv x_1(\bmod p)$及同余的性质4°，即得$f'(x_{\alpha-1})\equiv f'(x_1)(\bmod p)$，但$p\nmid f'(x_1)$，于是$p\nmid f'(x_{\alpha-1})$，故(b)

刚好有一个解

$$t_{\alpha-1}=t'_{\alpha-1}+pt_{\alpha},\quad t_{\alpha}=0,\ \pm1,\ \pm2,\ \cdots$$

因此把上式代入(a)，刚好给出(23)的一个解

$$x=x_{\alpha-1}+p^{\alpha-1}(t'_{\alpha-1}+pt_{\alpha})=x_{\alpha}+p^{\alpha}t_{\alpha},$$

其中 $x_{\alpha}=x_{\alpha-1}+p^{\alpha-1}t'_{\alpha-1}\equiv x_1 \pmod p$，故定理对 α 的情形亦正确.

定理4·9的证明方法提供了一种由(24)的解求出(23)的解的方法. 从上述内容，可以看到解高次同余式的问题，可归结为解素数模的高次同余式的问题.

例4·6 解同余式

$$f(x)=x^4+7x+4\equiv0 \pmod{27}$$

解 $f(x)\equiv0 \pmod 3$ 有且只有一个解 $x\equiv1 \pmod 3$，并且 $f'(1)\not\equiv0 \pmod 3$. 以 $x=1+3t_1$ 代入 $f(x)\equiv0 \pmod 9$，得

$$f(1)+3t_1f'(1)\equiv0 \pmod 9$$

但 $f(1)=12\equiv3 \pmod 9$，$f'(1)=11\equiv2 \pmod 9$，故

$$3+3t_1\times2\equiv0 \pmod 9,\ 即\ 2t_1+1\equiv0 \pmod 3.$$

因此 $t_1=1+3t_2$，而

$$x=1+3(1+3t_2)=4+9t_2\equiv4 \pmod 9$$

是 $f(x)\equiv0 \pmod 9$ 的一个解. 以 $x=4+9t_2$ 代入 $f(x)\equiv0 \pmod{27}$，即得

$$f(4)+9t_2f'(4)\equiv0 \pmod{27},$$

$$18+9t_2\cdot20\equiv0 \pmod{27},$$

即 $2t_2+2\equiv0 \pmod 3$，$t_2=2+3t_3$，故

$$x=4+9(2+3t_3)=22+27t_3\equiv22 \pmod{27}$$

是所求的解.

解合数模高次同余式的问题，归根到底是解素数模高次同余式的问题。为此下面着重研究素数模高次同余式的解法问题。

定理 4·10 同余式

$$f(x)\equiv 0(\bmod p),\ f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0 \quad (26)$$

其中p是素数，$a_n\not\equiv 0(\bmod p)$，与一个次数不超过$p-1$的素数p为模的同余式同解。

证明 由多项式的带余除法知，存在二整系数多项式$q(x)$及$r(x)$，使得

$$f(x)=(x^p-x)q(x)+r(x),\ \partial r(x)<p.$$

其中$\partial r(x)$表示$r(x)$的次数。由费马定理知道，对于任意整数x都有$x^p-x\equiv 0(\bmod p)$，所以对任何整数x都有

$$f(x)\equiv r(x)(\bmod p)$$

因此(26)与$r(x)\equiv 0(\bmod p)$同解。

例如，$f(x)=x^4+7x+4\equiv x^4+x+1(\bmod 3)$ (a)

$$x^4+x+1=(x^3-x)x+x^2+x+1,$$

$$\therefore\ f(x)\equiv x^2+x+1(\bmod 3) \quad (b)$$

与(a)同解，(b)有且只有一个解$x\equiv 1(\bmod 3)$，事实上，$x^2+x+1\equiv(x-1)^2(\bmod 3)$。

定理 4·11 设$k\leqslant n$，而$x\equiv\alpha_i(\bmod p)$，$i=1,\cdots,k$，是(26)的k个不同的解，则对任何整数x都有

$$f(x)\equiv(x-\alpha_1)\cdots(x-\alpha_k)f_k(x)(\bmod p) \quad (27)$$

其中$\partial f_k(x)=n-k$，且$f_k(x)$的首项系数是a_n。

证明 由多项式的带余除法，得

$$f(x)=(x-\alpha_1)f_1(x)+r,$$

其中$f_1(x)$是首项系数为a_n的$n-1$次整系数多项式，r是一个整数，由假设$f(\alpha_1)\equiv 0(\bmod p)$，故$r\equiv 0(\bmod p)$，因此

对任何整数x，都有

$$f(x)\equiv(x-\alpha_1)f_1(x)(\bmod p).$$

令$x=\alpha_i(i=2, \cdots, n)$得

$$0\equiv f(\alpha_i)\equiv(\alpha_i-\alpha_1)f_1(\alpha_i)(\bmod p),$$

但$\alpha_i\not\equiv\alpha_1(\bmod p)$，p 是素数，而素数模剩余类环是没有零因子的。故

$$f_1(\alpha_i)\equiv 0(\bmod p)(i=2, \cdots, k).$$

由此容易用数学归纳法来证明本定理。

系1 (i) 对任何整数x都有

$x^{p-1}-1\equiv(x-1)(x-2)\cdots[x-(p-1)](\bmod p)$;

(ii) (Wilson 定理)$(p-1)!+1\equiv 0(\bmod p)$。

证明 (i) 由费马定理知道，$x^{p-1}\equiv 1(\bmod p)$有$p-1$个不同的解：$x\equiv 1, 2, \cdots, p-1(\bmod p)$，再由定理4·11，得

$$x^{p-1}-1\equiv(x-1)(x-2)\cdots[x-(p-1)]g(x)(\bmod p),$$

其中$\partial g(x)=(p-1)-(p-1)=0$，且$g(x)\equiv 1(\bmod p)$。

(ii) 在(i)中取$x=0$，我们得到

$$-1\equiv(-1)(-2)\cdots[-(p-1)](\bmod p).$$

$$\therefore\quad(-1)^{p-1}(p-1)!+1\equiv 0(\bmod p).$$

当$p>2$时，$(-1)^{p-1}=1$，故$(p-1)!+1\equiv 0(\bmod p)$;
当$p=2$时，显然$(p-1)!+1=1+1\equiv 0(\bmod 2)$。

这个证法是拉格朗日（Lagrange）给出的。

系2 同余式(26)的解数（指不同解的个数）不超过它的次数。

证明 我们用反证法证明之，设（26）至少有$n+1$个解，

$$x\equiv\alpha_i(\bmod p), \quad i=1, 2, \cdots, n, n+1.$$

由定理4·11得

$$f(x)\equiv a_n(x-\alpha_1)\cdots(x-\alpha_n)(\bmod p),$$

由于$f(\alpha_{n+1})\equiv 0(\bmod p)$，所以

$$a_n(\alpha_{n+1}-\alpha_1)\cdots(\alpha_{n+1}-\alpha_n)\equiv 0(\bmod p),$$

但p为素数，$a_n\not\equiv 0(\bmod p)$，故有$-\alpha_i(0<i<n+1)$使$\alpha_{n+1}-\alpha_i\equiv 0(\bmod p)$，这与假设矛盾。

下面我们研究同余式(26)在什么条件下，它的解数与次数相等。因为$a_n\not\equiv 0(\bmod p)$，而模p的剩余类环是一个域，所以$\{a_n\}$有逆元$\{a_n'\}$，使得$\{a_n\}\{a_n'\}=\{1\}$（或者应用定理1·12亦可得到同样的结论），故存在a_n'使得$a_na_n'\equiv 1(\bmod p)$，把(26)的两边同乘以a_n'，得

$$x^n+(a_n'a_{n-1})x^{n-1}+\cdots+a_n'a_0\equiv 0(\bmod p), \qquad (26')$$

显然(26′)与(26)同解。

定理 4·12 若$n\leqslant p$，则同余式

$$f(x)\equiv 0(\bmod p),\ f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0 \qquad (28)$$

有n个解的充要条件是：以f(x)除x^p-x所得的余式的一切系数都是p的倍数。

证明 因为f(x)的首项系数是1，故由带余除法知有二整系数多项式q(x)及r(x)，使

$$x^p-x=f(x)q(x)+r(x), \qquad (29)$$

且$\partial r(x)<n$，$\partial q(x)=p-n$。

若(28)有n个解，由费马定理知道，这n个解都是$x^p-x\equiv 0(\bmod p)$的解，由(29)知道这些解也都是$r(x)\equiv 0(\bmod p)$的解，但$\partial r(x)<n$，由定理4·11的系2知道r(x)的系数都是p的倍数。

反之，若$r(x)$的系数都是p的倍数，则由(29)及费马定理知道，x为任何整数时，都有

$$f(x)q(x)\equiv 0(\bmod p) \tag{30}$$

这就是说(30)有p个不同的解$x\equiv 0, 1, \cdots, p-1(\bmod p)$。今设$f(x)\equiv 0(\bmod p)$的解数$k<n$，那么$q(x)\equiv 0(\bmod p)$的解数$p-k>p-n=\partial q(x)$，这与定理4·11的系2矛盾，所以$f(x)\equiv 0(\bmod p)$一定有$n$个不同的解。

必须注意，高次同余式$f(x)\equiv 0(\bmod p)$的$f(x)$是模m剩余类环上的多项式，它的根（即同余式的解）的个数，比起数域上多项式的根的个数复杂得多。若m是合数，由定理4·8知道它的根往往多于其次数n；当$m=p$为素数时，其解的个数就不大于n了。当$n\leqslant p$时，当且仅当(28)满足定理4·12的条件时，其不同解的个数才等于n。

习　题

1. 求下列各同余式的解：

(i) $256x\equiv 179(\bmod 337)$，337是素数；

(ii) $258x\equiv 131(\bmod 348)$；

(iii) $3x\equiv 10(\bmod 29)$；

(iv) $47x\equiv 89(\bmod 111)$；

(v) $660x\equiv 595(\bmod 1385)$；

(vi) $1215x\equiv 560(\bmod 2755)$。

2. 若$(2, m)=1$，则同余式

$$2^k x\equiv b(\bmod m)$$

有解，应用同余的性质7°，建立一种简单的解法。

3. 应用上题的方法解第一题(i)。

4. 仿照第二题的方法，写出下面同余式的一种简单解法：

$3^k x\equiv b(\bmod m)$，$(3, m)=1$ (a)

5. 用上题方法解第一题(iv)。

6. 设$(a, m)=1$，$1<a<m$，推广习题2，4的方法，证明要求得同余式

$$ax\equiv b \pmod m \qquad (1)$$

的解答，可以先从找出同余式$b+mt\equiv 0 \pmod p$（p是a的素因数）的解答着手，次应用同余的性质7°以求（1）的解。并用此法解同余式

$$1296x\equiv 1125 \pmod{1935}.$$

注：习题2、4、6为我们提供了一种较简单的解一元一次同余式的方法。

7. 应用同余的性质4°与10°，求下列联立同余式

$$\begin{cases} x+4y\equiv 29 \pmod{143} \\ 2x-9y\equiv 59 \pmod{143} \end{cases}$$

的解。

8. 若$ax\equiv b \pmod m$，且$(a, m)=1$，则这个同余式的唯一解用记号$x\equiv \frac{b}{a} \pmod m$来表示。求$\frac{1}{2}$，$\frac{1}{3}$，$\frac{1}{4}$，$\frac{1}{5}$，$\frac{1}{6} \pmod 7$.

9. 求：$\frac{1}{47} \pmod{93}$；$\frac{23}{37} \pmod{50}$；$\frac{49}{102} \pmod{121}$。

10. 导出下列诸公式：

(i) 若$(a, m)=(k, m)=1$，则$\frac{b}{a}\equiv \frac{bk}{ak} \pmod m$；

(ii) 若$(a_1, m)=(a_2, m)=1$，则

$$\frac{b_1}{a_1}\pm\frac{b_2}{a_2}\equiv \frac{a_2b_1\pm a_1b_2}{a_1a_2} \pmod m;$$

(iii) 若$(a_1, m)=(a_2, m)=1$，则

$$\frac{b_1}{a_1}\cdot\frac{b_2}{a_2}\equiv \frac{b_1b_2}{a_1a_2} \pmod m;$$

(iv) $\frac{b_1}{a_1}:\frac{b_2}{a_2}\equiv \frac{b_1a_2}{a_1b_2} \pmod m$，

其中a_1，a_2，b_2都与m互素，且$\frac{b_1}{a_1}:\frac{b_2}{a_2}$是同余式$\frac{b_2}{a_2}x\equiv \frac{b_1}{a_1} \pmod m$的解。

11. 应用例3·7，证明定理4·1.

12. 求下列同余式组的解：

(i) $\begin{cases} x\equiv 3(\mathrm{mod}\ 7), \\ x\equiv 5(\mathrm{mod}\ 11); \end{cases}$ (ii) $\begin{cases} x\equiv 2(\mathrm{mod}\ 11), \\ x\equiv 5(\mathrm{mod}\ 7), \\ x\equiv 4(\mathrm{mod}\ 5); \end{cases}$

(iii) $\begin{cases} x\equiv 1(\mathrm{mod}\ 7), \\ 3x\equiv 4(\mathrm{mod}\ 5), \\ 8x\equiv 4(\mathrm{mod}\ 9). \end{cases}$

13. 解下列各题（杨辉《续古摘奇算法》(1275)）：

(i) 七数剩一，八数剩二，九数剩四，问本数；

(ii) 二数余一，五数余二，七数余三，九数余五，问本数；

(iii) 十一数余三，七十二数余二，十三数余一，问本数.

14. 证明，同余式组

$$\begin{cases} x\equiv a(\mathrm{mod}\ m_1) \\ x\equiv a(\mathrm{mod}\ m_2) \end{cases} \quad (\alpha)$$

的全部解是：$x\equiv a(\mathrm{mod}\ [m_1,\ m_2])$. (β)

15. 若$n_i | m_i (n=1,\ \cdots,\ k)$，其中$(n_i,\ n_j)=1$，$(i\neq j=1,\ \cdots,\ k)$，且

$[n_1,\ n_2,\ \cdots,\ n_k]=[m_1,\ m_2,\ \cdots,\ m_k]$，则有解的同余式组

$$x\equiv b_i(\mathrm{mod}\ m_i)\ (i=1,\ 2,\ \cdots,\ k) \quad (a)$$

的解与同余式组

$$x\equiv b_i(\mathrm{mod}\ n_i)\ (i=1,\ 2,\ \cdots,\ k) \quad (b)$$

的解相同.

此题的结论，给我们一种用孙子定理解符合定理4·6条件的同余式组(a)的方法.

16.

(i) 解 $\begin{cases} x\equiv 2(\mathrm{mod}\ 7), \\ x\equiv 5(\mathrm{mod}\ 9), \\ x\equiv 11(\mathrm{mod}\ 15). \end{cases}$

(ii) 今有数不知总，以五累减之无剩，以七百一十五累减之剩十，以二百四十七累减之剩一百四十，以三百九十一累减之剩二百四十五，以一百八十七累减之剩一百零九，问总数若干？（黄宗宪：《求一术通解》

17. 甲、乙两港的距离不超过5000公里，今有三只轮船于某天零时从甲港开往乙港，假定三只轮船每天24小时都是匀速航行，若干天后的零时第一只轮船首先到达，几天后的18时，第二只轮船也到达，几天后的8时，第三只轮船也到达了。假若每天第一只轮船走300公里，第二只轮船走240公里，第三只轮船走180公里，问甲、乙两港实际距离是多少公里？三只轮船各走多长时间？

18. 应用定理4·11，关于模7分解下列多项式为因式（对于模7用验算法去求它们的根）

(i) $3x^4+x^3+5x-2$； (ii) $2x^3+5x^2-2x-3$；

(iii) x^4-2x^2+x+4.

19. 对于模11分解下列多项式为因式：

(i) $2x^4+x^3-3x-2x-2$； (ii) x^4+x+4.

20. 求下列同余式的解：

(i) $x^7-6\equiv 0 \pmod 5$； (ii) $x^8-2x^7+x^5-x^4-x+3\equiv 0 \pmod 5$； (iii) $6x^3+27x^2+17x+20\equiv 0 \pmod{30}$；

(iv) $31x^4+57x^3+96x+191\equiv 0 \pmod{225}$.

21. 应用定理4·12判别：(i) $x^2+2x-1\equiv 0 \pmod 7$ 是否有两个不同的解；(ii) $x^3+x-3\equiv 0 \pmod 7$ 是否有三个不同的解。

22. 设 n 个未知数的同余式组：

$$\begin{aligned} &a_{11}x_1+a_{12}x_2+\cdots+a_{1n}x_n\equiv b_1,\\ &a_{21}x_1+a_{22}x_2+\cdots+a_{2n}x_n\equiv b_2,\\ &\cdots\qquad\cdots\qquad\cdots,\\ &a_{k1}x_1+a_{k2}x_2+\cdots+a_{kn}x_n\equiv b_k \end{aligned} \pmod m \qquad (1)$$

令 $l_i=a_{i1}x_1+a_{i2}x_2+\cdots+a_{in}x_n-b_i$，以 $c_1l_1+c_2l_2+\cdots+c_kl_k\equiv 0 \pmod m$ $(c_i, m)=1$，代替 $l_i\equiv 0 \pmod m$，所得的新同余式组

(2)，证明(2)与(1)同解。

应用上述结论，仿照解线性方程组的方法，

解

$$\begin{cases} 2x+y-z\equiv 5, \\ 3x-2y+z\equiv 4, \quad (\bmod 9) \\ x+2y-3z\equiv 6. \end{cases}$$

23．歌诀：

“元宵佳节闹盈盈，来往观灯街上行，
上下灯球光闪灼，几遭绕走数难清，
从头五数恰无零，七数二瓯犹无停，
九数之数剩四盏，红灯几盏放光明。”

答曰310盏，解之。

24．应用22题的结论来破译密码．若其解答矩阵是

$$\begin{pmatrix} 2 & 1 & -1 \\ 3 & -2 & 1 \\ 1 & 2 & -3 \end{pmatrix} (\bmod 29)$$

其对应关系如下：

—, a, b, c, … v, w, x, y, z, *, *.

0, 1, 2, 3, … 22, 23, 24, 25, 26, 27, 28.

在密码上写一个字“victor”求出它的解答．

25．设$n\nmid p-1$，$n>1$，$(a, p)=1$．证明同余式

$$x^n\equiv a(\bmod p)$$

有解的充要条件是$a^{\frac{p-1}{n}}\equiv 1(\bmod p)$，并且有解时，就有n个解．

26．设n是正整数，$(a, m)=1$，并且已知同余式$x^n\equiv a\ (\bmod m)$有一解$x\equiv x_0(\bmod m)$，证明这同余式的一切解，可以表成

$$x\equiv yx_0(\bmod m).$$

其中y是同余式$y^n\equiv 1(\bmod m)$的解．

第五章　二次同余式与平方剩余

本章的目的是比较深入地讨论二次同余式，并把它归结为讨论形如

$$x^2 \equiv a \pmod{m}$$

的同余式，从而引入平方剩余和平方非剩余的概念，再应用勒让得（Legendre）符号和雅可比（Jacobi）符号（两个常用的数论函数）去讨论当模$m=p$为素数时$(a,\ p)=1$的a是否二次剩余；进而研究m为合数的情况，最后再应用本章的知识来解决两个不定方程的问题，简单介绍华林(Waring)问题。

第一节　一般二次同余式

形如　　$ax^2+bx+c\equiv 0 \pmod{m}\ a\not\equiv 0 \pmod{m}$　　(1)

的m是自然数的整系数同余式，叫做二次同余式（quadratic congruences）。

一个二次同余式，可能没有解，如$x^2-3\equiv 0 \pmod{7}$没有解；也可能解的数目多于2，$x^2-1\equiv 0 \pmod{8}$，就有$x\equiv 1,\ 3,\ 5,\ 7 \pmod{8}$四个解。所以首先要讨论(1)什么时候有解，其次研究解的数量与解法的问题。

设$m=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$是它的标准分解式，则由定理4·8知道，(1)与同余式组

$$ax^2+bx+c\equiv \pmod{p_i^{\alpha_i}}\ (i=1,\ \cdots,\ k)\qquad (2)$$

同解，并且若(2)的第i个同余式关于模$p_i^{\alpha_i}$的解数为T_i

时，则(1)关于模m的解数为：

$$T = T_1 T_2 \cdots T_K.$$

因此，我们首先应讨论(2)的每一个同余式是否有解，次考虑

$$f(x) = ax^2 + bx + c \equiv 0 (\bmod p^\alpha) \qquad (3)$$

若$p^\alpha \mid (a, b, c)$，则任一整数都满足(3)，即(3)有解，且其解数是P^α．若$p^r \parallel (a, b, c)$（表示$p^r \mid (a, b, c)$，而$p^{r+1} \nmid (a, b, c)$），$r < \alpha$，则可先解同余式

$$\frac{a}{p^r}x^2 + \frac{b}{p^r}x + \frac{c}{p^r} \equiv 0 (\bmod P^{\alpha - r}) \qquad (3)'$$

这里$p \nmid (\frac{a}{p^r}, \frac{b}{p^r}, \frac{c}{p^r})$．所以研究(3)的解时，可设$p \nmid (a, b, c)$。

(i) 若$p \mid (a, b)$，则$p \mid c$，这时同余式

$$f(x) \equiv 0 (\bmod p)$$

没有解，事实上，任给x_0都有$p \mid ax_0^2 + bx_0$，$p \nmid c \Longrightarrow p \nmid ax_0^2 + bx_0 + c$。

(ii) 若$p \nmid a$，$p \nmid b$，则$f'(x) = 2ax + b \equiv 0 (\bmod p)$无解，因此由定理4·9知道，(3)有解的充要条件是

$$ax^2 + bx + c \equiv 0 (\bmod p)$$

有解．因为上面的同余式实际就是$bx + c \equiv 0 (\bmod p)$，而$(p, b) = 1$，由定理4·1知其有解，因此(3)亦有解。

(iii) 若$p \nmid a$，$p > 2$，则$(p^\alpha, 4a) = 1$，用4a乘(3)后再配方，即得

$$(2ax + b)^2 - A \equiv 0 (\bmod p^\alpha), \quad A = b^2 - 4ac, \qquad (4)$$

显然(4)与(3)同解，用y代$2ax + b$，得

$$y^2 - A \equiv 0 (\bmod p^\alpha) \qquad (5)$$

现在证明（3）有解的充要条件是（5）有解．上面的讨论，实际上已证明了必要性。

下面证明其充分性，设（5）有解$y\equiv y_0(\bmod p^{\alpha})$，即$y_0^2-A\equiv 0(\bmod p^{\alpha})$。因为$(2a, p^{\alpha})=1$，所以

$$2ax+b\equiv y_0(\bmod p^{\alpha})$$

有解$x\equiv x_0(\bmod p^{\alpha})$，即$2ax_0+b\equiv y_0(\bmod p^{\alpha})$、

$\therefore$ $(2ax_0-b)^2-A\equiv 0(\bmod p^{\alpha})$，即（3）有解$x\equiv x_0$ $(\bmod p^{\alpha})$。

(iv) 最后讨论，$p=2$，$2\nmid a$的情形。若$2\nmid b$，则$f'(x)=2ax+b\equiv 0(\bmod 2)$无解，与(ii)的讨论一样，即知（3）有解的充要条件是

$$ax^2+bx+c\equiv 0(\bmod 2)$$

有解。并由费马定理知道，对于任何x都有$x^2\equiv x(\bmod 2)$，用x替换上同余式的x^2，得到与上式同解的同余式

$$(a+b)x+c\equiv 0(\bmod 2),$$

但是$2|a+b$，故（3）有解的充要条件是$2|c$。

若$2|b$，则可设$b=2b_1$，此时由于$(2^{\alpha}, a)=1$，故同余式（3）与同余式

$$(ax)^2+2b_1(ax)+ac=(ax+b_1)^2-A\equiv 0(\bmod 2^{\alpha}) \tag{4'}$$

同解，其中$A=b_1^2-ac$。仿(iii)可以证明(4′)有解的充要条件是

$$y^2-A\equiv 0(\bmod 2^{\alpha}),\ y=ax+b, \tag{5'}$$

有解。

总之，要判断一个一般二次同余式（3）是否有解，一定可以化为判断形如（5）（包括(5′)）的同余式是否有解。

今转而讨论(5)，若 $P^{\alpha}|A$，则(5)成为

$$y^2\equiv 0(\bmod P^{\alpha}),$$

容易求出它的一切解。

若$p^{\alpha}\nmid A$，则设$p^{\beta}\parallel A(\alpha>\beta\geqslant 0$，$\Longrightarrow A=p^{\beta}A_1$，$p\nmid A_1$。若$\beta>0$，则(5)有解的必要条件是：$p|y$，设$p^{\gamma}\,|\,y\Longrightarrow y=p^{\gamma}t$，$p\nmid t$。若$p=p^{\gamma}$是(5)的解，则代入(5)得

$$p^{2\gamma}t^2-p^{\beta}A_1\equiv 0(\bmod p^{\alpha}),\quad p\nmid t^2,\quad p\nmid A_1. \qquad (6)$$

由(6)知$p^{2\gamma}=(p^{2\gamma}t^2,\ p^{\alpha})=(p^{\beta}A_1,\ p^{\alpha})=p^{\beta}$，

$$\therefore\qquad 2\gamma=\beta.$$

这说明了，只有当β是偶数时，(5)才可能有解，至于$\beta=2\gamma$为偶数时，(5)是否有解，还要看

$$t^2-A\equiv 0(\bmod p^{\alpha-\beta}),\ (A_1,\ p^{\alpha-\beta})=1,$$ 有没有解而定。

综上所述，要讨论一般二次同余式有没有解的问题，归结为讨论二次同余式

$$x^2\equiv a(\bmod p^{\alpha}),\ (a,\ p^{\alpha})=1 \qquad (7)$$

有没有解的问题，或者更一般地，讨论

$$x^2\equiv a(\bmod m),\ (a,\ m)=1, \qquad (8)$$

有没有解。为此我们引入

定义5·1 若同余式(8)有解，则 a 叫做模m的平方剩余或二次剩余（quadratic residue)；若(8)无解，则a叫做模m的平方非剩余或二次非剩余（quadratic non-residue)。

第二节　奇素数的平方剩余和平方非剩余

本节只讨论奇素数p(本章无特别说明p都表示奇素数)的平方剩余和平方非剩余，即讨论形如

$$x^2 \equiv a(\bmod p),\quad (a, p)=1 \tag{9}$$

的同余式的解。

由定理4·11系2知道，(9)若有解时，只有两个解。事实上，若$x_0^2 \equiv a(\bmod p)$，则$(-x_0)^2 \equiv a(\bmod p)$并且$x_0 \not\equiv -x_0(\bmod p)$，因为不然的话，$2x_0 \equiv 0(\bmod p)$，而$(P,2)=1$，$(p, x^0)=1 \Longrightarrow (p, 2x_0)=1$，这是不可能的。

在模P的互素剩余系

$$-\frac{p-1}{2},\ \cdots,\ -1,\ 1,\ \cdots,\ \frac{p-1}{2} \tag{10}$$

中，有且只有$\frac{p-1}{2}$个是平方剩余，即与

$$(\pm 1)^2,\ (\pm 2)^2,\ \cdots,\ (\pm \frac{p-1}{2})^2$$

同余的$\frac{p-1}{2}$个数，这些数关于模P是两两互不同余的，因为若$k^2 \equiv l^2(\bmod p)$，$0<k<l\leqslant\frac{p-1}{2}$，则$x^2 \equiv l^2(\bmod p)$，在模p的互素剩余系(10)中有4个解$x=-l, l, -k, k$，这与定理4·11系2的结论矛盾. 此外(10)中另$\frac{p-1}{2}$个数，都不与任何一个数的平方同余，所以(10)中有$\frac{p-1}{2}$个数目是平方剩余，$\frac{p-1}{2}$个数目是平方非剩余. 从而得到

定理5·1　模p的互素剩余系(10)中有$\frac{p-1}{2}$个数目

是模p的平方剩余，$\frac{p-1}{2}$个数目是模p的平方非剩余。

定理5·2 （欧拉判别条件）如果（a，p）=1，a是模p的平方剩余，那末

$$a^{\frac{p-1}{2}} \equiv 1 \pmod p; \tag{11}$$

而如果a是模p的平方非剩余，那末

$$a^{\frac{p-1}{2}} \equiv -1 \pmod p. \tag{12}$$

证明 由费马定理知道，当（a，p）=1时，有

$$a^{p-1} \equiv 1 \pmod p,$$

即 $a^{p-1}-1=(a^{\frac{p-1}{2}}-1)(a^{\frac{p-1}{2}}+1)\equiv 0 \pmod p$。

因为p是奇素数，所以上式右边必有一因子被p整除，并且只有一因子被p整除。因为如果二因子都被p整除，那末

$$p \mid [(a^{\frac{p-1}{2}}-1)+(a^{\frac{p-1}{2}}+1)] \Longrightarrow p \mid 2,$$

这是不可能的。所以对于任何(a，p)=1的a来说，同余式(11)和(12)有且只有一个成立。

但是对于所有的平方剩余a，总有一个x_0使得

$$x_0^2 \equiv a \pmod p.$$

因为$(x_0, p)=1$，$x_0^{p-1} \equiv (\bmod p)$，所以把上式的两边$\frac{p-1}{2}$次乘方，就得到(11)。这就是说(10)中的$\frac{p-1}{2}$个平方剩余都是(11)的解，并且由定理4·11系2知道(11)的解数不多于$\frac{p-1}{2}$。由费马定理知$a^{p-1}\equiv 1 \pmod p$有(p-1)个解，所以(10)中另$\frac{p-1}{2}$个数都是(12)的解（模p的平方

非剩余）。

因为平方剩余和平方非剩余是排中的，所以定理5·2实际包含下列四命题．在$(a, p)=1$的前提下，

a满足(11)$\underset{\text{逆}}{\overset{\text{正}}{\Longleftrightarrow}}$a是模P的平方剩余；

a不满足(11)〔即a满足(12)〕$\underset{\text{否}}{\overset{\text{否}}{\Longleftrightarrow}}$a是模p的平方非剩余。

例5·1 求出模13的平方剩余和平方非剩余。

解 $(\pm1)^2\equiv1$，$(\pm2)^2\equiv4$，$(\pm3)^2\equiv-4$，$(\pm4)^2\equiv3$，$(\pm5)^2\equiv-1$，$(\pm6)^2\equiv-3 \pmod{13}$，所以$-4$，$-3$，$-1$，1，3，4是模13的平方剩余，$-6$，$-5$，$-2$，2，5，6是模13的平方非剩余。

系 若a是模p的平方剩余，则同余式(9)刚好有两个解。

此系是定理4·11系2的直接结论．但亦可用4·12及欧拉判别条件，证明如下：

证明∵ $x^{p-1}-a^{\frac{p-1}{2}}=(x^2)^{\frac{p-1}{2}}-a^{\frac{p-1}{2}}$，

∴ $x^2-a \mid x^{p-1}-a^{\frac{p-1}{2}}$，

当a是模p的平方剩余时，$a^{\frac{p-1}{2}}\equiv1 \pmod p$，所以用$x^2-a$除$x^{p-1}-1$时，其余式的系数都是p的倍数，由定理4·12知(9)刚好有两个解。

第三节　勒 让 得 符 号

上节虽然介绍了用欧拉判别条件来判别a是否p的平方剩余的方法，但当p相当大时，用起来确有困难，为了判别

的方便，本节引入勒让得符号.

定义5·2 符号$\left(\frac{a}{p}\right)$叫做a关于p的勒让得符号（Legendre's symlol），这个符号是对于给定的奇素数p，定义在一切整数a上的函数，它的值规定如下：

$$\left(\frac{a}{p}\right)=\begin{cases}1, & \text{若}a\text{是模}p\text{的平方剩余；}\\ -1, & \text{若}a\text{是模}p\text{的平方非剩余；}\\ 0, & \text{若}p\mid a.\end{cases}$$

由定义 5·2 可以看出，若能迅速地计算出$\left(\frac{a}{p}\right)$的值，就可确定a是否模p的平方剩余．也就可以知道，同余式

$$x^2\equiv a(\bmod p)$$

是否有解．下面先讨论勒让得符号的一些性质，由定理5·2立即得到：

1° $\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}}(\bmod p)$.

2° 若$a_1\equiv a_2(\bmod p)$，则$\left(\frac{a_1}{p}\right)=\left(\frac{a_2}{p}\right)$.

3° $\left(\frac{1}{p}\right)=1$.

证明 $1=1^2$因此1是模p的平方剩余.

性质1°中取$a=-1$，立得

4° $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$.

因为当p是形如$4m+1$的素数时，$\frac{p-1}{2}$是偶数；而当p是形如$4m+3$的素数时，$\frac{p-1}{2}$是奇数．所以对于形如$4m+1$的素数-1是平方剩余，对于形如$4m+3$的素数-1是平方非剩余.

5° $\left(\frac{a_1a_2\cdots a_n}{p}\right)=\left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\cdots\left(\frac{a_n}{p}\right)$.

证明 由性质1°，得

$$\left(\frac{a_1a_2\cdots a_n}{p}\right)\equiv(a_1a_2\cdots a_n)^{\frac{p-1}{2}}=a_1^{\frac{p-1}{2}}a_2^{\frac{p-1}{2}}\cdots a_n^{\frac{p-1}{2}}$$

$$\equiv\left(\frac{a_1}{p}\right)\left(\frac{a_2}{p_2}\right)\cdots\left(\frac{a_n}{p}\right)(\text{mod } p).$$

$\therefore$ $\left(\frac{a_1a_2\cdots a_n}{p}\right)=\left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\cdots\left(\frac{a_n}{p}\right)$.

从5°立即可得

6° 若$(b, p)=1$，则$\left(\frac{ab^2}{p}\right)=\left(\frac{a}{p}\right)$.

勒让得符号横线上面的字母亦称分子，下面的字母亦称分母，但$\frac{a}{p}$不是分数，不过借用分子、分母的词汇而已。性质6°指出，勒让得符号的分子里可以去掉任意的平方因子。

为了得出勒让得符号的进一步性质，我们来讨论同余式组：令$p_1=\frac{p-1}{2}$，$(a, p)=1$

$$\begin{cases}a\cdot 1\equiv\varepsilon_1\gamma_1(\text{mod } p),\\ \cdots\cdots\cdots\\ a\cdot p_1\equiv\varepsilon_{p_1}\gamma_{p_1}(\text{mod } p).\end{cases}$$

其中$\varepsilon_t\gamma_t$是$at(t=1, \cdots, P_1)$的绝对最小剩余，而$0\leqslant\gamma_t\leqslant p_1$，$\varepsilon_t=\pm1$，并且(14)各式的右边是关于模p互不同余的$p_1$个数。否则，若

$\varepsilon_i\gamma_i\equiv\varepsilon_j\gamma_j$ $(\text{mod } p)\Longrightarrow a\cdot i\equiv a\cdot j$ $(\text{mod } p)\Longrightarrow i\equiv j$ $(\text{mod } p)$，这是不可能的。由定理3·5系2知道，数目

$a\cdot 1$，$-a\cdot 1$，$a\cdot 2$，$-a\cdot 2$，$\cdots$，ap_1，$-ap_1$

是模p的一个互素剩余系．它们的绝对最小剩余分别是

$\varepsilon_1\gamma_1$，$-\varepsilon_1\gamma_1$，$\varepsilon_2\gamma_2$，$-\varepsilon_2\gamma_2$，…，$\varepsilon_{p_1}\gamma_{p_1}$，$-\varepsilon_{p_1}\gamma_{p_1}$。

该叙列中的正值γ_1，γ_2，…，γ_{p_1}是1，2，…，p_1的一个排列，所以把同余式组(14)的两边乘起来，并约掉$p_1!=\gamma_1\gamma_2\cdots\gamma_{p_1}$，得

$$a^{\frac{p-1}{2}}\equiv\varepsilon_1\varepsilon_2\cdots\varepsilon_{p_1}(\mathrm{mod}\ p)。$$

从而得到

7° 若ε_1，ε_2，…，ε_{p_1}是同余式组(14)中的数目（+1或−1），则

$$\left(\frac{a}{p}\right)=\varepsilon_1\varepsilon_2\cdots\varepsilon_{p_1}.$$

由性质7°及数论函数“〔〕”，可以求出勒让得符号最完善的表示式．事实上，在(14)中，当 at 的最小正剩余大于p_1时，$\varepsilon_t=-1$，这时$\left[\frac{2at}{p}\right]=2k+1$；当at的最小正剩余$\leqslant p_1$时，$\varepsilon_t=1$，这时$\left[\frac{2at}{p}\right]=2l$，即$\varepsilon_t=(-1)^{\left[\frac{2at}{p}\right]}$．因而

$$\varepsilon_1\varepsilon_2\cdots\varepsilon_{p_1}=(-1)^{\sum\limits_{t=1}^{p_1}\left[\frac{2at}{p}\right]},$$

故得

8° 若$(a,p)=1$，则$\left(\frac{a}{p}\right)=(-1)^{\sum\limits_{t=1}^{p_1}\left[\frac{2at}{p}\right]}$． (15)

9° 若a是奇数，$(a,p)=1$，则

$$\left(\frac{2}{p}\right)\left(\frac{a}{p}\right)=(-1)^{\sum\limits_{t=1}^{p_1}\left[\frac{at}{p}\right]+\frac{p^2-1}{8}}$$

证明 因为$a+p$是偶数，由性质2°知

$$\left(\frac{2a}{p}\right)=\left(\frac{2a+2p}{p}\right)=\left(\frac{4\times\frac{a+p}{2}}{p}\right)\overset{6°}{=\!=}\left(\frac{\frac{a+p}{2}}{p}\right)$$

$$\overset{8°}{=\!=}(-1)^{\sum\limits_{t=1}^{p_1}\left[\frac{(a+p)t}{p}\right]}$$

$$=(-1)^{\sum\limits_{t=1}^{p_1}\left[\frac{at}{p}\right]+\sum\limits_{t=1}^{p_1}t}.$$

而$\sum\limits_{t=1}^{p_1}t=1+2+\cdots\frac{p-1}{2}=\frac{p^2-1}{8}$，代入上式的右边，就得到所要的结论。

性质9°的等式中，取$a=1$，得

10° $$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}} \tag{16}$$

因为$\frac{(8m\pm1)^2-1}{8}=8m^2\pm2m$是偶数，$\frac{(8m\pm3)^2-1}{8}=8m^2\pm6m+1$是奇数。从而推得，2是形如$8m\pm1$的素数的平方剩余；是形如$8m\pm3$的素数的平方非剩余。即

11° 对奇素数p，

$$\left(\frac{2}{P}\right)=\begin{cases}1，当p=8m\pm1时；\\-1，当p=8m\pm3时。\end{cases}$$

由性质9°及10°立即得到比(15)计算量少的

12° 当$(a, p)=1$，a是奇数时，

$$\left(\frac{a}{p}\right)=(-1)^{\sum\limits_{t=1}^{p_1}\left[\frac{at}{p}\right]}. \tag{17}$$

要注意(17)与(15)的差别．例如，

$$\left(\frac{7}{13}\right)\overset{12°}{=\!=\!=}(-1)^{\sum\limits_{t=1}^{6}\left[\frac{7t}{13}\right]}=(-1)^{9}=-1;$$

$$\left(\frac{7}{13}\right)\overset{8°}{=\!=\!=}(-1)^{\sum\limits_{t=1}^{6}\left[\frac{14t}{13}\right]}=(-1)^{1+2+3+4+5+6}$$

$$=(-1)^{21}=-1.$$

$$\left(\frac{6}{13}\right)\overset{8°}{=\!=\!=}(-1)^{\sum\limits_{t=1}^{6}\left[\frac{12t}{13}\right]}=-1,$$

若改用性质12°的(17)式，则$\left(\frac{6}{13}\right)=(-1)^{\sum\limits_{t=1}^{6}\left[\frac{6t}{13}\right]}=1$，

这是错误的．

定理5·3 （二次反转定律～quadratic reciprocity law ～）如果p和q都是奇素数，$(p, q)=1$,则

$$\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right). \tag{18}$$

(18)是表示p与q相互的平方剩余的关系，当且仅当p，q都是$4m+3$形的奇素数时，

$$\left(\frac{q}{p}\right)=-\left(\frac{p}{q}\right).$$

当p与q中至少有一个是4m+1形的奇素数时，

$$\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right).$$

证明　令$p_1=\frac{p-1}{2}$，$q_1=\frac{q-1}{2}$，$S_1=\sum_{x=1}^{p_1}\left[\frac{qx}{p}\right]$

$$S_2=\sum_{y=1}^{q_1}\left[\frac{py}{q}\right].$$

由性质12°知，当p，q是奇数时，有

$$\left(\frac{q}{p}\right)=(-1)^{S_1}，\left(\frac{p}{q}\right)=(-1)^{S_2}\Longrightarrow\left(\frac{q}{p}\right)=(-1)^{S_1+S_2}\left(\frac{p}{q}\right),$$

今只需证明$S_1+S_2=p_1q_1$即可。

讨论p_1q_1个数对（qx，py），$x=1，2，\cdots，p_1$，$y=1，2，\cdots，q_1$。因为$(q，y)=1$，所以不可能有$py=qx$的情况出现。令$p_1q_1=S_1'+S_2'$，其中S_1'是满足$py<qx$的数对（qx，py）的个数，S_2'是满足$py>qx$的数对(qx，py)的个数。因而S_1'是适合$y<\frac{q}{p}x$的数对的个数。当给定一个x值之后，就有$y=1，2，\cdots，\left[\frac{q}{p}x\right]$时，都满足不等式$py<qx$，亦即对给定的x，满足$py<qx$的数对（qx，py）有$\left[\frac{q}{p}x\right]$个。同理当给定一个y值之后，满足不等式$qx<py$的数对（qx，py）有$\left[\frac{p}{q}y\right]$个。

$$\therefore \quad S_1' = \sum_{x=1}^{p_1}\left[\frac{qx}{p}\right] = S_1, \quad S_2' = \sum_{y=1}^{q_1}\left[\frac{py}{q}\right] = S_2.$$

亦即

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right).$$

二次反转定律的证明方法是有多种多样的，这里的证明所用的基础知识比较少。

1783年欧拉首先发现二次反转定律，但是没有证明它，1785年勒让得重新发现这个定律，并予以证明，但其证法不够理想，1790年他倡议引入今天所谓的勒让得符号，把二次反转定律表示成，当p，q是不同的奇素数时，则

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

1798年高斯（Gauss）首先严格地证明了二次反转定律。他首先用完全归纳法证明了这个结论，并刊登在高斯1801年出版的名著《Disquisitions arithmetical》（《算学的研究》）中，后来高斯又给出这个定律的六种证法，这里的证法就是其中的一种略加简化而已，六种证法之后他又给出多种证法，到现在这个定理的证法共有50种左右。

有了二次反转定理，可简化勒让得符号的计算。

例5·2 计算：(i) $\left(\frac{438}{593}\right)$；(ii) $\left(\frac{2023}{1231}\right)$。其中593 1231都是素数。

解 (i) 因为438＝2·3·73，由性质5°得

$$\left(\frac{438}{593}\right) = \left(\frac{2}{593}\right)\left(\frac{3}{593}\right)\left(\frac{73}{593}\right),$$

下面分别算出右边三个勒让得符号。因为$593=8\times74+1$，所以由性质10°得

$$\left(\frac{2}{593}\right)=1;$$

$$\left(\frac{3}{593}\right)=(-1)^{\frac{593-1}{2}\cdot\frac{3-1}{2}}\left(\frac{593}{3}\right)=\left(\frac{593}{3}\right)\overset{2^\circ}{=\!=}$$

$$\left(\frac{2}{3}\right)=(-1)^{\frac{3^2-1}{8}}=-1.$$

$$\left(\frac{73}{593}\right)=\left(\frac{593}{73}\right)\overset{2^\circ}{=\!=}\left(\frac{9}{73}\right)=\left(\frac{3^2}{73}\right)\overset{5^\circ}{=\!=}1.$$

$$\therefore\left(\frac{438}{593}\right)=-1.$$

即同余式 $x^2\equiv438\pmod{593}$ 无解。

因为$438\equiv-155\pmod{593}$，所以此题亦可计算如下：由性质2°、4°、5°、定理5·3及$593=4\times148+1$得

$$\left(\frac{438}{593}\right)=\left(\frac{-155}{593}\right)=\left(\frac{-1}{593}\right)\left(\frac{5}{593}\right)\left(\frac{31}{593}\right)$$

$$=(-1)^{\frac{593-1}{2}}\left(\frac{593}{5}\right)\left(\frac{593}{31}\right)=\left(\frac{3}{5}\right)\left(\frac{4}{31}\right)$$

$$=\left(\frac{5}{3}\right)=\left(\frac{2}{3}\right)=-1.$$

(ii) $$\left(\frac{2033}{1231}\right)=\left(\frac{792}{1231}\right)=\left(\frac{2^3}{1231}\right)\left(\frac{3^2}{1231}\right)\left(\frac{11}{1231}\right)$$

$$=\left(\frac{2}{1231}\right)\left(\frac{11}{1231}\right).$$

因为$1231=8\times153+7$，所以由性质10°知$\left(\frac{2}{1231}\right)=1$。

$\therefore \quad \left(\frac{2033}{1231}\right)=\left(\frac{11}{1231}\right)=-\left(\frac{1231}{11}\right)=-\left(\frac{-1}{11}\right)=(-1)^{\frac{11-1}{2}}$

$=1$。即 $x^2\equiv 792 \pmod{1231}$ 有解。

第四节 雅可比符号

在计算勒让得符号的时候，最大的困难是把分子分解成素因子的乘积，当数目很大时，甚至是无法分解的，为了避免这个困难，雅可比把勒让得符号推广到，当分母是奇合数的情况。

定义5·3 设m是大于1的奇数，而且 $m=p_1p_2\cdots p_r$ 是它的素因子分解式（这些因子之间可以有相等的），则雅可比符号（Jacobi's symbol）$\left(\frac{a}{m}\right)$是定义在一切整数a上的函数，其函数值是由下面等式给出：

$$\left(\frac{a}{m}\right)=\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_r}\right),$$

右边是勒让得符号．

显然（a，m）=d>1时，$\left(\frac{a}{m}\right)=0$，许多书中定义5·2和5·3都排除了a与p或m不互素的情况，即增加一个条件（a，p）=1或（a，m）=1。

必须注意，雅可比符号一方面是勒让得符号的推广，另一方面又有一个重要的差别，即勒让得符号$\left(\frac{a}{p}\right)$可用以判别a是否模p的二次剩余，即 $x^2\equiv a \pmod p$ 是否有解．但是雅可比符号，当m是合数时，就没有这个功用了。例如，因为$\left(\frac{2}{3}\right)=-1$，$x^2\equiv 2 \pmod 3$无解，所以 $x^2\equiv 2$（mod

9）亦无解，而$\left(\frac{2}{9}\right)=\left(\frac{2}{3}\right)\left(\frac{2}{3}\right)=(-1)^2=1$。

雅可比符号有下列诸性质：

1° 若$a_1\equiv a_2 \pmod m$，则$\left(\frac{a_1}{m}\right)=\left(\frac{a_2}{m}\right)$。

证明 可由定义5·3及勒让得符号的性质2°，当$m=p_1p_2\cdots p_r$时，得到

$$\left(\frac{a_1}{m}\right)=\left(\frac{a_1}{p_1}\right)\left(\frac{a_1}{p_2}\right)\cdots\left(\frac{a_1}{p_r}\right)=\left(\frac{a_2}{p_1}\right)\left(\frac{a_2}{p_2}\right)\cdots\left(\frac{a_2}{p_r}\right)$$
$$=\left(\frac{a_2}{m}\right).$$

由定义5·3及勒让得符号的性质3°，得

2° $\left(\frac{1}{m}\right)=1$。

3° $\left(\frac{-1}{m}\right)=(-1)^{\frac{m-1}{2}}$.

证明 设$m=p_1p_2\cdots p_r$（下面无特别声明，m都用此式表示）。由定义5·3及勒让得符号性质4°等，以及$2q_i=p_i-1$（$i=1,\cdots,r$），得

$$\left(\frac{-1}{m}\right)=\left(\frac{-1}{p_1}\right)\left(\frac{-1}{p_2}\right)\cdots\left(\frac{-1}{p_r}\right)$$
$$=(-1)^{\frac{p_1-1}{2}+\frac{p_2-1}{2}+\cdots+\frac{p_r-1}{2}}$$
$$=(-1)^{q_1+q_2+\cdots+q_r}.$$

而 $$\frac{m-1}{2}=\frac{p_1p_2\cdots p_r-1}{2}=\frac{(1+2q_1)(1+2q_2)\cdots(1+2q_r)-1}{2}$$
$$=q_1+q_2+\cdots+q_r+2N.$$

$$\therefore \quad \left(\frac{-1}{m}\right)=(-1)^{\frac{m-1}{2}}.$$

4° $\left(\frac{a_1a_2\cdots a_n}{m}\right)=\left(\frac{a_1}{m}\right)\left(\frac{a_2}{m}\right)\cdots\left(\frac{a_n}{m}\right).$

证明 $\left(\frac{a_1a_2\cdots a_n}{m}\right)=\left(\frac{a_1a_2\cdots a_n}{p_1}\right)\left(\frac{a_1a_2\cdots a_n}{p_2}\right)\cdots$

$$\left(\frac{a_1a_2\cdots a_n}{p_r}\right)=\left\{\left(\frac{a_1}{p_1}\right)\left(\frac{a_1}{p_2}\right)\cdots\left(\frac{a_1}{p_r}\right)\right\}\left\{\left(\frac{a_2}{p_1}\right)\right.$$

$$\left.\left(\frac{a_2}{p_2}\right)\cdots\left(\frac{a_2}{p_r}\right)\right\}\cdots\left\{\left(\frac{a_n}{p_1}\right)\left(\frac{a_n}{p_2}\right)\cdots\left(\frac{a_n}{p_r}\right)\right\}=$$

$$\left(\frac{a_1}{m}\right)\left(\frac{a_2}{m}\right)\cdots\left(\frac{a_n}{m}\right).$$

5° 若 $(b, m)=1$，则$\left(\frac{ab^2}{m}\right)=\left(\frac{a}{m}\right).$

6° $\left(\frac{2}{m}\right)=(-1)^{\frac{m^2-1}{8}}.$

最后可把勒让得符号的二次反转定律推广于雅可比符号，这样就可以回避了分子因子分解的困难。

定理5·4 设m和n是大于1的二奇数，则

$$\left(\frac{n}{m}\right)=(-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}\left(\frac{m}{n}\right).$$

证明 当$(m, n)\neq 1$时，$\left(\frac{m}{n}\right)=\left(\frac{n}{m}\right)=0$，故定理成立。当$(m, n)=1$时，设$m=p_1\cdots p_r$，$n=q_1\cdots q_s$（因子之间可以相等的），则

$$\left(\frac{n}{m}\right)=\left(\frac{n}{p_1}\right)\cdots\left(\frac{n}{p_r}\right)=\prod_{\alpha=1}^{r}\prod_{\beta=1}^{s}\left(\frac{q_\beta}{p_\alpha}\right)=$$

$$=(-1)^{\sum\limits_{\alpha=1}^{r}\sum\limits_{\beta=1}^{s}\frac{p_\alpha-1}{2}\cdot\frac{q_\beta-1}{2}}\prod_{\alpha=1}^{r}\prod_{\beta=1}^{s}\left(\frac{p_\alpha}{q_\beta}\right)=$$

$$=(-1)^{\left(\sum\limits_{\alpha=1}^{\gamma}\frac{p_\alpha-1}{2}\right)\left(\sum\limits_{\beta=1}^{s}\frac{q_\beta-1}{2}\right)}\left(\frac{m}{n}\right)=$$

$$=(-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}\left(\frac{m}{n}\right).$$

因为在性质3°的证明中知道

$$\sum_{\alpha=1}^{r}\frac{p_\alpha}{2}=\frac{m-1}{2}-2N,\quad \sum_{\beta=1}^{s}\frac{q_\beta-1}{2}=\frac{n-1}{2}-2N'.$$

例5·3 计算：(i) $\left(\frac{853}{1409}\right)$，(ii) $\left(\frac{5381}{6277}\right)$.

解 (i) $\left(\frac{853}{1409}\right)=\left(\frac{1409}{853}\right)=\left(\frac{556}{853}\right)=$

$$=\left(\frac{2^2}{853}\right)\left(\frac{139}{853}\right)=\left(\frac{139}{853}\right)=\left(\frac{853}{139}\right)=$$

$$=\left(\frac{19}{139}\right)=-\left(\frac{139}{19}\right)=-\left(\frac{6}{19}\right)=$$

$$=-\left(\frac{2}{19}\right)\left(\frac{3}{19}\right)=\left(\frac{3}{19}\right)=-\left(\frac{19}{3}\right)=$$

$$=-\left(\frac{1}{3}\right)=-1.$$

(ii) $\left(\frac{5381}{6277}\right)=\left(\frac{-896}{6277}\right)=\left(\frac{-1}{6277}\right)\left(\frac{2^7}{6277}\right)$

$$\left(\frac{7}{6277}\right)=-\left(\frac{6277}{7}\right)=-\left(\frac{-2}{7}\right)=$$

$$= -\left(\frac{-1}{7}\right)\left(\frac{2}{7}\right) = \left(\frac{2}{7}\right) = 1.$$

例5·4 判断同余式

$x^2 \equiv 286 \pmod{563}$ 及 $x^2 \equiv 219 \pmod{383}$ 是否有解。

解　因为563，383都是素数，故可以用雅可比符号判别之。

$$\left(\frac{286}{563}\right) = \left(\frac{2}{563}\right)\left(\frac{143}{563}\right) = (-1)^{\frac{563^2-1}{8}} \cdot$$

$$(-1)^{\frac{143-1}{2}\cdot\frac{563-1}{2}}\left(\frac{563}{143}\right) = \left(\frac{-9}{143}\right) = \left(\frac{-1}{143}\right) =$$

$$(-1)^{\frac{143-1}{2}} = -1,$$

所以 $x^2 \equiv 286 \pmod{563}$ 无解。

$$\left(\frac{219}{383}\right) = -\left(\frac{383}{219}\right) = -\left(\frac{164}{219}\right) = -\left(\frac{2^2}{219}\right)\left(\frac{41}{219}\right)$$

$$= -\left(\frac{41}{219}\right) = -\left(\frac{219}{41}\right) = -\left(\frac{14}{41}\right)$$

$$= -\left(\frac{2}{41}\right)\left(\frac{7}{41}\right) = -\left(\frac{7}{41}\right) = -\left(\frac{41}{7}\right)$$

$$= -\left(\frac{-1}{7}\right) = -(-1)^{\frac{7-1}{2}} = 1,$$

所以 $x^2 \equiv 219 \pmod{383}$ 有解。

下面谈谈同余式(9)的实际解法。自然当模p给定后，亦可试验 $\pm 1, \pm 2, \cdots, \pm\frac{p-1}{2}$ 中有否(9)的解，但是当p充分大时，这是不可能的，因此至今的解法都借助于查表，下面将介绍两个由欧拉判别条件（定理5·2）直接得到的同余式(9)的解的普遍公式。

Ⅰ．设 $p=4m+3$，则 $\frac{p-1}{2}=2m+1$，当 $\left(\frac{a}{p}\right)=1$ 时，由欧拉判别条件(11)，得

$$a^{2m+1}\equiv 1\ (\mathrm{mod}\ p)$$

因为 $(a,\ p)=1$，以 a 乘上同余式的两边，得

$$a^{2m+2}\equiv a(\mathrm{mod}\ p)\Longrightarrow(a^{m+1})^2\equiv a(\mathrm{mod}\ p)$$

$$\therefore\qquad x\equiv\pm a^{m+1}(\mathrm{mod}\ p)$$

是(9)的解。

Ⅱ．设 $p=8m+5$，则 $\frac{p-1}{2}=4m+2$，当 $\left(\frac{a}{p}\right)=1$ 时，由(11)得

$$a^{4m+2}\equiv 1(\mathrm{mod}\ p)\Longrightarrow(a^{2m+1}+1)(a^{2m+1}-1)\equiv 0(\mathrm{mod}\ p)$$

$$\Longrightarrow p\,|\,a^{2m+1}+1 \text{或} p\,|\,a^{2m+1}-1 \text{之一，}$$

但不能同时整除此二式。否则，$p\,|\,(a^{m+1}+1)-(a^{m+1}-1)\Longrightarrow p\,|\,2$，这是不可能的。于是有下列两种情况之一发生：

（1） 若 $a^{2m+1}-1\equiv 0(\mathrm{mod}\ p)\Longrightarrow(a^{m+1})^2\equiv a(\mathrm{mod}\ p)$，即 $x\equiv\pm a^{m+1}(\mathrm{mod}\ p)$ 是(9)的解。

（2） 若 $a^{2m+1}+1\equiv 0(\mathrm{mod}\ p)\Longrightarrow(a^{m+1})^2\equiv -a\ (\mathrm{mod}\ p)$ 因此，我们要找到一个模 p 的平方非剩余 f 来，用 $f^{4m+2}\equiv -1(\mathrm{mod}\ p)$ 乘上同余式，得

$$(a^{m+1}f^{2m+1})^2\equiv a(\mathrm{mod}\ p)$$

所以 $x\equiv\pm a^{m+1}f^{2m+1}(\mathrm{mod}\ p)$ 是(9)的解。

由于 $p=8m+5$，故 2 是模 p 的平方非剩余（勒让得符号的性质11°），故(9)的解是：

$$x\equiv\pm 2^{2m+1}a^{m+1}(\mathrm{mod}\ p).$$

但是必须注意，当 p 很大时，这种解法仍不方便。

Ⅲ．当 $p=8m+1$ 时，用上述方法是无法求出(9)的解的。其解法要用下一章"指数"的知识，且需查表：

苏联数学家阿·恩·柯尔金（А·Н·Коркин）创造了一种方法，并借助特制的一种表，来解形如

$$x^n \equiv a \pmod p \tag{19}$$

的同余式。下面介绍当 $p=8k+1$ 的素数时，同余式（9）的柯尔金解法（即(19)中 $n=2$ 的情况）。

柯尔金引理 设 $p=2^\lambda k+1$，$\lambda \geqslant 3$，k 是奇数，则同余式

$$z_1^2 \equiv -1,\ z_2^{2^2} \equiv -1,\ \cdots,\ z_{\lambda-1}^{2^{\lambda-1}} \equiv -1 \pmod p \tag{20}$$

依次有 $2,\ 2^2,\ \cdots,\ 2^{\lambda-1}$ 个不同的解，并且前一个同余式的解可由后一个同余式的解经平方而得到。

证明 设 f 是模 p 的平方非剩余，由(12)有

$$f^{\frac{p-1}{2}} = f^{2^{\lambda-1}k} \equiv -1 \pmod p, \tag{21}$$

即

$$(f^{2^{\lambda-2}k})^2 \equiv -1 \pmod p. \tag{21$'$}$$

所以 $z_1 \equiv U_{11} \equiv f^{2^{\lambda-2}k}$，$U_{12} \equiv -U_{11} \pmod p$ 是(20)第一式的两个不同解。事实上，若 $U_{11} \equiv U_{12} \pmod p$，则 $2f^{2^{\lambda-2}k} \equiv 0 \pmod p$，而 $p \nmid 2$，$p \nmid f$，所以这是不可能的。

今把(21)改写为

$$(f^{2^{\lambda-3}k})^{2^2} \equiv -1 \pmod p, \tag{21$''$}$$

因此，$z_2 \equiv U_{21} \equiv f^{2^{\lambda-3}k}$ $U_{22} \equiv -U_{21} \pmod p$ 是(20)第二式的两个解；又因为

$$U_{21}^{2^2} \equiv -1,\ U_{11}^{2^2} \equiv 1,\ U_{12}^{2^2} \equiv 1 \pmod p,$$

$\therefore\quad U_{23}\equiv U_{11}U_{21}$，$U_{24}\equiv U_{12}U_{21}\equiv -U_{11}U_{21}\equiv -U_{23}$ $(\bmod p)$亦(20)第二式的两个解。且U_{21}，U_{22}，U_{23}，U_{24}是(20)第二式的四个不同的解。事实上，若

$$U_{21}\equiv \pm U_{23}(\bmod p)\Longrightarrow U_{21}\equiv \pm U_{11}U_{21}(\bmod p)$$

$$\Longrightarrow U_{11}\equiv \pm 1(\bmod p)\Longrightarrow U_{11}^2\equiv 1(\bmod p)$$

这与$U_{11}^2\equiv -1(\bmod p)$矛盾．其他情况亦可类似地 证 明。

一般地，要求(20)的第μ($\mu<\lambda$)个同余式

$$z_\mu^{2^\mu}\equiv -1(\bmod p)$$

的全部解，可把(21)改写为

$$(f^{2^{\lambda-\mu-1}k})^{2^\mu}\equiv -1(\bmod p) \qquad (21)^{(\mu)}$$

因此，$z_\mu\equiv U_{\mu 1}\equiv f^{2^{\lambda-\mu-1}k}$，$U_{\mu 2}\equiv -U_{\mu 1}(\bmod p)$，以及$U_{\mu 1}$与(20)中第一至第$\mu-1$个同余式的解之积，都 是 $(20)^{(\mu)}$ 的解，并且这些解关于模 p是互不同余的．也就是$(21)^{(\mu)}$还有如下的$2+2^2+\cdots+2^{\mu-1}=2^\mu-2$个解：

$U_{\mu 3}\equiv U_{11}U_{\mu 1}$，$U_{\mu 4}\equiv U_{12}U_{\mu 1}$，$U_{\mu 5}\equiv U_{21}U_{\mu 1}$，$\cdots$，$U_{\mu 8}\equiv U_{24}U_{\mu 1}$，$\cdots$，$U_{\mu,2^\mu}\equiv U_{\mu-1,2^{\mu-1}}\cdot U_{\mu 1}(\bmod p)$； 其 中无两个关于模 p是同余的。因为，若对于小于μ的ξ，ρ有

$U_{\mu 1}U_{\xi\eta}\equiv U_{\mu 1}U_{\rho\sigma}(\bmod p)\Longrightarrow U_{\xi\eta}\equiv U_{\rho\sigma}(\bmod p)$这是不可能的．事实上，若$\xi=\rho$，$\eta\neq\sigma$，则$U_{\xi\eta}$与$U_{\rho\sigma}$是(20)第$\xi$式的两个不同的解；若$\xi\neq\rho$，可设$\xi<\rho$，则

$$(U_{\rho\sigma})^{2^\rho}\equiv -1(\bmod p),$$

$$(U_{\xi\eta})^{2^\rho}=[(U_{\xi\eta})^{2^\xi}]^{2^{\rho-\xi}}\equiv(-1)^{2^{\rho-\xi}}=1(\bmod p).$$

∴ $U_{\xi\eta} \not\equiv U_{\rho\sigma} \pmod p$.

类似地，可证$U_{\mu 1}$，$U_{\mu 2}$与其他诸解关于模 p 亦不同余。

最后，证明引理的后一部分，显然

$$U_{\mu 1}, \ U_{\mu 2}, \ \cdots, \ U_{\mu, \ 2^{\mu}} \qquad (\alpha)$$

中每一个的平方，都是(20)第 $\mu-1$ 个同余式的解，即它必与

$$U_{\mu-1, \ 1}, \ U_{\mu-1, \ 2}, \ \cdots, \ U_{\mu-1, \ 2^{\mu-1}} \qquad (\beta)$$

之一关于模p同余，要求

$$U_{\mu\eta}^2 \equiv U_{\mu\sigma}^2 \pmod p$$

成立，应有

$$(U_{\mu\eta} - U_{\mu\sigma})(U_{\mu\eta} + U_{\mu\sigma}) \equiv 0 \pmod p,$$

因为 $\eta \neq \sigma$，所以只能是

$$U_{\mu\eta} \equiv -U_{\mu\sigma} \pmod p.$$

也就是说，(α)中仅有两个数（即 $\pm U_{\mu\eta}$）的平方同对应于(β)的一个数；所以(β)的任一数都可以由（α）的某个数经平方而得到。

柯尔金把(20)中所有同余式的解的绝对最小剩余，称为数 p 的平方特征（square characteristic），他曾就5000以内的素数p造出它们的平方特征表来。克·阿·波瑟(K·A·Поссе）继续造出10000以内的 p 的平方特征表。上面(α)、(β)分别是数 p 的第μ、$\mu-1$组的平方特征，并且已知(β)的每一个数都可由(α)的某一数平方而得到。

定理5·5 设$p = 2^{\lambda} k + 1, \lambda \geqslant 3, k$为奇数，$\left(\frac{a}{p}\right) = 1$，则

$$x^2 \equiv a \pmod p \qquad (a)$$

有且只有下列三种情况之一：

（1） 当$a^k \equiv 1 \pmod p$时，其解为：

$$x \equiv \pm a^{\frac{k+1}{2}} \pmod p;$$

（2） 当 $a^k \equiv -1 \pmod p$ 时，f 是模 p 的任一平方非剩余，则其解为：

$$x \equiv \pm f^{2^{\lambda-2}k} a^{\frac{k+1}{2}} \pmod p;$$

（3） 当 $a^{2^{\lambda-s}k} \equiv -1 \pmod p$，$2 \leqslant s \leqslant \lambda$，$a^k \equiv b^2 \pmod p$，其中 b 是数 p 的某一第 $\lambda - s + 1$ 组的平方特征，$bt \equiv 1 \pmod p$ 时，则（9）的解是：

$$x \equiv \pm a^{\frac{k+1}{2}} t \pmod p.$$

证明 因为 $\left(\frac{a}{p}\right) = 1$，由欧拉判别条件，有

$$a^{\frac{p-1}{2}} = a^{2^{\lambda-1}k} \equiv 1 \pmod p.$$

先证明：要吗就是 $a^k \equiv 1 \pmod p$；要吗就是在数列

$$a^{2^{\lambda-2}k},\ a^{2^{\lambda-3}k},\ \cdots,\ a^{2k},\ a^k$$

中，有一个数关于模 p 与 -1 同余．因为

$$a^{2^{\lambda-1}k} - 1 = (a^{2^{\lambda-2}k} - 1)(a^{2^{\lambda-2}k} + 1) \equiv 0 \pmod p,$$

左边二因式中，有且只有一个数被 p 除尽。

若 $p \mid a^{2^{\lambda-2}k} + 1$，则论断已被证明。

若 $p \mid a^{2^{\lambda-2}k} - 1$，则 $p \mid (a^{2^{\lambda-3}k} + 1)(a^{2^{\lambda-3}k} - 1)$

重复上面的讨论，若 $p \mid a^{2^{\lambda-3}k} + 1$，则论断已被证明。若

$$p \mid a^{2^{\lambda-3}k}-1 \Longrightarrow p \mid (a^{2^{\lambda-4}k}+1)(a^{2^{\lambda-4}k}-1)$$

$\Longrightarrow \cdots$，即$p \mid a^{2^{\lambda-s}k}+1$（$s=2$，…，$\lambda$中之一），或$p \mid a^k-1$。这就证明了所要的结论。

下面分三种情况：

（1）$a^k \equiv 1 \pmod p \Longrightarrow a^{k+1}=\left(a^{\frac{k+1}{2}}\right)^2$

$$\equiv a \pmod p,$$

$$\therefore\ x \equiv \pm a^{\frac{k+1}{2}} \pmod p \text{ 是（9）的解。}$$

（2）$a^k \equiv -1 \pmod p \Longrightarrow \left(a^{\frac{k+1}{2}}\right)^2 \equiv -a$ $\pmod p$，设f是模p的一个平方非剩余，即

$$f^{\frac{p-1}{2}}=f^{2^{\lambda-1}k} \equiv -1 \pmod p \Longrightarrow \left(f^{2^{\lambda-2}k}a^{\frac{k+1}{2}}\right)^2$$

$$\equiv a \pmod p,$$

$$\therefore \quad x \equiv \pm f^{2^{\lambda-2}k}a^{\frac{k+1}{2}} \pmod p$$

是同余式（9）的解。

（3）$a^{2^{\lambda-s}k} \equiv -1 \pmod p$，$2 \leqslant s < \lambda$，

即 $(a^k)^{2^{\lambda-s}} \equiv -1 \pmod p$。

因此，a^k是（20）中第（$\lambda-s$）个同余式的一个解（即数p的第$\lambda-s$组平方特征中的一个），并且由柯尔金引理知道

$$a^k \equiv b^2 \pmod p \qquad (22)$$

里的b是（20）中第（$\lambda-s+1$）个同余式的一个解，以a乘（22）的两边，得

$$\left(a^{\frac{k+1}{2}}\right)^2 \equiv a\ b^2 \pmod p.$$

因为$(b,p)=1$，所以可以求出$bt\equiv 1 \pmod p$的解t，并得

$$\left(a^{\frac{k+1}{2}}t\right)^2\equiv a \pmod p,$$

$$\therefore \qquad x\equiv \pm a^{\frac{k+1}{2}}t \pmod p$$

是同余式（9）的解。

综合上述，我们得到，奇素数p为模的二次同余式（9）解的公式如下：

Ⅰ．$p=4m+3$时，$x\equiv \pm a^{m+1} \pmod p$；

Ⅱ．$p=8m+3$时，

（1） 当$a^{2m+1}\equiv 1 \pmod p$时，$x\equiv \pm a^{m+1} \pmod p$；

（2） 当$a^{2m+1}\equiv -1 \pmod p$时，$x\equiv \pm 2^{2m+1}a^{m+1}$ $\pmod p$；

Ⅲ．$p=8m+1=2^{\lambda}k+1$，$\lambda\geqslant 3$，k是奇数时，

（1） 当$a^k\equiv 1 \pmod p$时，$x\equiv \pm a^{\frac{k+1}{2}} \pmod p$；

（2） 当$a^k\equiv -1 \pmod p$时，

$$x\equiv \pm f^{2^{\lambda-2}k}a^{\frac{k+1}{2}} \pmod p,$$

其中$\left(\frac{f}{p}\right)=-1$；

（3） 当$a^{2^{\lambda-s}k}\equiv -1 \pmod p$，$2\leqslant s<\lambda$，$a^k\equiv b^2 \pmod p$，$bt\equiv 1 \pmod p$，其中b是（20）的第$\lambda-s+1$式的某一个解，则

$$x\equiv \pm a^{\frac{k+1}{2}}t \pmod p$$

是（9）的解。

例5·5 解下诸同余式

(i) $x^2 \equiv 11 \pmod{43}$； (ii) $x^2 \equiv 7 \pmod{29}$；

(iii) $x^2 \equiv 23 \pmod{101}$； (iv) $x^2 \equiv 2 \pmod{17}$；

(v) $x^2 \equiv 5 \pmod{41}$。

解 (i) $\left(\frac{11}{43}\right) = -\left(\frac{43}{11}\right) = -\left(\frac{-1}{11}\right) = 1$，所以该同余式有解，而$43 = 4 \times 10 + 3$，由情形Ⅰ，$m = 10$，$m + 1 = 11$，于是$x \equiv \pm 11^{11} \pmod{43}$是$x^2 \equiv 11 \pmod{43}$的解，经如下的计算：

$$11^2 \equiv -8 \pmod{43}, \quad 11^4 \equiv 21 \pmod{43},$$
$$11^8 \equiv 11 \pmod{43}, \quad 11^{10} \equiv -2 \pmod{43},$$
$$11^{11} \equiv 21 \pmod{43}.$$

所以$x \equiv \pm 21 \pmod{43}$是它的解

(ii) $\because \left(\frac{7}{29}\right) = \left(\frac{29}{7}\right) = \left(\frac{1}{7}\right) = 1$，

故该同余式有解，而$29 = 8 \times 3 + 5$，由情形Ⅱ，$a^{2m+1} = 7^7 \equiv 1 \pmod{29}$，所以

$$x \equiv \pm 7^4 \equiv \mp 6 \pmod{29}$$

是$x^2 \equiv 7 \pmod{29}$的解

(iii) $\because \left(\frac{23}{101}\right) = \left(\frac{101}{23}\right) = \left(\frac{9}{23}\right) = 1$，

而$101 = 8 \times 12 + 5$，$m = 12$，$2m + 1 = 25$，$m + 1 = 13$，经计算，$23^{25} \equiv -1 \pmod{101}$，由情形Ⅱ的（2）得

$$x \equiv \pm 2^{2m+1} \cdot 23^{m+1} = \pm 2^{25} \cdot 23^{13} \equiv \pm 10 \times 49$$
$$\equiv \mp 15 \pmod{101}$$

是$x^2 \equiv 23 \pmod{101}$的解。

(iv) $\because \left(\frac{2}{17}\right) = 1$，$17 = 2^4 \times 1 + 1$，$\lambda = 4$，

$k=1$，我们有（20）的同余式

$$z_1^2\equiv-1,\ z_2^4\equiv-1,\ z_3^8\equiv-1\ (\bmod\ 17) \qquad (a)$$

这里取 $f=-3$ 是模17的平方非剩余，根据欧拉判别条件，$(-3)^8\equiv-1\ (\bmod\ 17)$；$(-3)^4\equiv-4\ (\bmod\ 17)$，因此

$$u_{11}=f^{2^{\lambda-2}k}=(-3)^4\equiv-4,\ u_{12}=4\ (\bmod\ 17)$$

是（a）中第一个同余式的解，而

$$u_{21}\equiv f^{2^{\lambda-3}k}=(-3)^2\equiv-8,\ u_{22}\equiv8\ (\bmod\ 17),$$

$$u_{23}\equiv(-4)(-8)\equiv-2,\ u_{24}\equiv4\times(-8)\equiv2\ (\bmod 17)$$

是（a）中第二个同余式的解。最后

$$u_{31}\equiv f^{2^{\lambda-4}k}=f\equiv-3,\ u_{32}\equiv3,\ u_{33}\equiv u_{11}u_{31}\equiv-5,$$

$$u_{34}\equiv5,\ u_{35}\equiv u_{21}u_{31}\equiv7,\ u_{36}\equiv-7,\ u_{37}\equiv6,$$

$$u_{38}\equiv-6\ (\bmod 17)$$

是（a）第三式的解

今回头研究

$$x^2\equiv2\ (\bmod 17).$$

因为 $a^{2^2}=2^4\equiv-1\ (\bmod\ 17)$，由情形Ⅱ（3），$a^k=2\equiv2\ (\bmod 17)$ 是（a）里第 $\lambda-s=4-2=2$ 个同余式的一个解（即 u_{24}），所以在（a）的第三个同余式的解中可以找到一个 b，使得 $b^2\equiv2\ (\bmod 17)$，事实上 $b=u_{37}=6$，$6t\equiv1\ (\bmod\ 17)$ 有解 $t\equiv3\ (\bmod 17)$，所以

$$x\equiv\pm a^{\frac{k+1}{2}}t=\pm2\times3=\pm6\ (\bmod 17)$$

是 $x^2\equiv2\ (\bmod 17)$ 的解。实际上，此题不用上述方法亦可直接观察出上述结论。

（v） 因为$\left(\frac{5}{41}\right)=1$，$41=2^3\times5+1$，故$k=5$，$\lambda=3$，我们有（20）的同余式

$$z_1^2\equiv-1,\ z_2^{2^2}\equiv-1\pmod{41}$$

不难验证$\left(\frac{3}{41}\right)=-1$，故取$f=3$，仿（iv）的方法求其解为：$z_1\equiv\pm9$；$z_2\equiv\pm3$，$\pm14\pmod{41}$。

其次，因为$a^k=5^5\equiv9\pmod{41}$，$a^{2k}\equiv-1\pmod{41}$，故用情形Ⅱ（3）的方法，$a^k\equiv b^2\pmod{41}$，即$b\equiv3\pmod{41}$，而$3t\equiv1\pmod{41}$有解$t\equiv14\pmod{41}$。

又因$a^{\frac{k+1}{2}}\equiv5^3\equiv2\pmod{41}$，

∴ $$x\equiv\pm(2\times14)\equiv\mp13\pmod{41}$$

是$x^2\equiv5\pmod{41}$的解。

这里还应引起读者注意的是：本节虽已给出了模p的二次同余式的一般解法及解的公式，但是当p相当大时，还应借助平方特征表，才能求解，否则计算量太大。

第五节 合数模二次同余式

以上各节我们讨论了奇素数模的同余式

$$x^2\equiv a\pmod{p},(a,p)=1$$

有解的条件及其解法。本节将讨论合数模同余式

$$x^2\equiv a\pmod{m},\ (a,m)=1 \qquad (23)$$

有解的条件及解的个数和求解的方法

从定理4·8知道，若$m=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$是m的标准分解式，则（23）等价于同余式组

$$x^2\equiv a\left(\bmod p_i^{\alpha_i}\right)(i=1,\cdots,r). \qquad (24)$$

并且若用T_i表示（24）的第 i 个同余式的解数，则（23）的解数$T=T_1T_2\cdots T_r$，为此下面仅着重研究 p 为奇素数时，同余式

$$x^2\equiv a(\bmod p^\alpha),\ \alpha>0,\ (a,\ p)=1 \quad (25)$$

的解的存在条件，解法和解的数量。

定理5·6 当 p 是奇素数时，（25）有解的充要条件是：$\left(\frac{a}{p}\right)=1$，并且在有解的情况下，（25）有且只有两个解。

证明 必要性：若$\left(\frac{a}{p}\right)=-1$，则 $x^2\equiv a(\bmod p)$无解，于是（25）亦无解。否则，若$x\equiv x_1(\bmod p^\alpha)$是（25）的解，则

$$p^\alpha \mid x_1^2-a \Longrightarrow p \mid x_1^2-a \Longrightarrow x_1^2\equiv a(\bmod p) \Longrightarrow \left(\frac{a}{p}\right)$$

$=1$。这与$\left(\frac{a}{p}\right)=-1$的假设矛盾。

充分性：若$\left(\frac{a}{p}\right)=1$，由定理5·2的系知道$x^2\equiv a(\bmod p)$刚好有两个解，设$x\equiv x_1(\bmod p)$是它的一个解，那末由$(a,\ p)=1$，得$(x_1,\ p)=1$，又因$(2,\ p)=1$，得$(2x_1,\ p)=1$。

令$f(x)=x^2-a$，则$p\nmid f'(x_1)$。从定理4·9知由$x\equiv x_1(\bmod p)$可得（25）的唯一的一个解，所以（25）有且只有两个解。

下面讨论当$p=2$时，同余式

$$x^2\equiv a(\bmod 2^\alpha),\ \alpha>0,\ (2,\ a)=1 \quad (26)$$

有解的条件、解法及解的数量。

显然，当$\alpha=1$时，（26）对于任何 a 都有且只有一个

解，因此下面只讨论 $\alpha>1$ 的情况.

定理5·7 设 $\alpha>1$，则（26）有解的必要条件是：（i） 当 $\alpha=2$ 时，$a\equiv1\pmod 4$；（ii） 当 $\alpha\geqslant3$ 时，$a\equiv1\pmod 8$。

若上述条件成立，则（26）有解；并且当 $\alpha=2$ 时，其解数是2，当 $\alpha\geqslant3$ 时，其解数是4。

证明 若 $x\equiv x_1\pmod{2^\alpha}$ 是（26）的任一解，由 $(2,a)=1$，得 $(x_1,2)=1$，于是 $x_1=1+2t_1$，其中 t_1 是整数，代入（26）得

$$1+4t_1(t_1+1)\equiv a\pmod{2^\alpha}$$

（i） 当 $\alpha=2$ 时，$2^\alpha=4$，由上式得

$$a\equiv1\pmod 4;$$

（ii） 当 $\alpha\geqslant3$ 时，则

$$1+4t_1(t_1+1)\equiv a\pmod{2^\alpha}\Longrightarrow1+4t_1(t_1+1)\equiv a\pmod 8\Longrightarrow a\equiv1\pmod 8.$$

这就证明了条件的必要性。

反之，（i） 当 $\alpha=2$，$\alpha\equiv1\pmod 4$ 时，（26）有

$$x\equiv1,\ 3\pmod 4$$

两个解，且只有这两个解。

（ii） 当 $\alpha=3$，$a\equiv1\pmod 8$ 时，显然（26）有且只有四个解：

$x_3\equiv1$，$-x_3\equiv7$，$(x_3+4)\equiv5$，$-(x_3+4)\equiv3\pmod 8$，或者写作：

$x_{31}\equiv1$，$x_{32}\equiv-x_{31}\equiv7$，$x_{33}\equiv5$，$x_{34}\equiv-x_{33}\equiv3\pmod 8$。

也就是说，一切奇数都是 $x^2\equiv1\pmod 8$ 的解，可把

它统一写成

$$x=\pm(1+4t_3),\ t_3=0,\ \pm1,\ \pm2,\ \cdots. \quad (27)$$

事实上，$t_3=0$时，(27)表示x_3，$-x_3$二解，$t=1$时，(27)表示$\pm(x_3+4)$二解，t的其他值都是重复出现上述情况。

在$\alpha>3$的情况，(27)中取t_3的不同值亦可把一切奇数对模2^α进行分类。如$\alpha=4$时，取$t=0, 1, -1, 2$时，(27)依次表示

$x\equiv1, 15$；$x\equiv5, 11$；$x\equiv13, 3$；$x\equiv9, 7 \pmod{16}$，其中$x\equiv1, 15, 9, 7 \pmod{16}$是$x^2\equiv1 \pmod{16}$的解，$x\equiv5, 11, 13, 3 \pmod{16}$是$x^2\equiv9 \pmod{16}$的解。对于模16奇数的类有且只有八个，故t的其他值都是重复上述的结果，一般地

(iii) 当$\alpha>3$，$a\equiv1 \pmod 8$时，只须考察(27)的$2^{\alpha-1}$个类中，那些适合

$$x^2\equiv a \pmod{2^\alpha}$$

其中$a\equiv1, 9, \cdots, 1+(2^{\alpha-3}-1)\times8 \pmod{2^\alpha}$。

当$\alpha=4$时，必须

$(1+4t_3)^2\equiv1+8t_3\equiv a \pmod{2^4} \Longrightarrow t_3'$

$\equiv\dfrac{a-1}{8} \pmod 2 \Longrightarrow t_3=t_3'+2t_4$，$t_3'=\dfrac{a-x_3^2}{8}$

$=\dfrac{a-1}{8}$，

把$t_3=t_3'+2t_4$代入(27)，得

$x=\pm(1+4t_3'+8t_4)=\pm(x_4+8t_4)$，$t_4=0, \pm1$，其中$x_4=1+4t_3'$，当$a\equiv1 \pmod{16}$，$t_3'=0$，$\cdots(27)'$

则$x^2\equiv1 \pmod{16}$有且只有四个解$x\equiv\pm1, \pm7 \pmod{16}$；

当 $a\equiv9(\bmod 16)$时，$t_3'=1$，则 $x^2\equiv9(\bmod 16)$有且只有四个解 $x\equiv\pm5$，$\pm3(\bmod 16)$，即当$a\equiv1(\bmod 8)$时，$x^2\equiv a(\bmod 2^4)$有且只有四个解. $x\equiv\pm x_4$，$\pm(x_4+8)(\bmod 16)$，(因为当 $t_4=2k$ 时，$x_4+8t_4=x_4+16k\equiv x_4(\bmod 16)$；当 $t_4=2k+1$ 时，$x_4+8t_4=x_4+16k+8\equiv x_4+8(\bmod 16)$。

依此类推，当 $\alpha=5$，$a\equiv1(\bmod 8)$时，适合同余式

$$x^2\equiv a(\bmod 2^5) \qquad (s)$$

的一切整数是：

$$x=\pm(x_5+16t_5),\ t_5=0,\ \pm1,\ \pm2,\ \cdots, \qquad (27'')$$

其中 $x_5=x_4+8t_4'$，$t_4'=\frac{a-x_4^2}{16}$。与前面一样，易证(s)有且只有四个解：

$$x\equiv\pm x_5,\ \pm(x_5+16)(\bmod 32)\ .$$

一般地，当 $a\equiv1(\bmod 8)$时，适合同余式(26)的一切整数是：

$$x=\pm(x_\alpha+2^{\alpha-1}t_\alpha);\ t_\alpha=0,\ \pm1,\ \pm2,\ \cdots.$$

(27‴) 其中 $x_\alpha=x_{\alpha-1}+2^{\alpha-2}t'_{\alpha-1}$，

$t'_{\alpha-1}=\frac{a-x_{\alpha-1}^2}{2^{\alpha-1}}$。故(26)有且只有四个解：

$$x\equiv\pm x_\alpha,\ \pm(x_\alpha+2^{\alpha-1})(\bmod 2^\alpha).$$

$\because$ $x_\alpha\equiv x_{\alpha-1}\equiv\cdots\equiv x_3\equiv1(\bmod 4)$；$x_\alpha+2^{\alpha-1}\equiv x_2\equiv1(\bmod 4)$，$-(x_\alpha+2^{\alpha-1})\equiv-x_\alpha\equiv-1(\bmod 4)$.

$\therefore$ $x_\alpha\not\equiv-x_\alpha$；$x_\alpha+2^{\alpha-1}\not\equiv-(x_\alpha+2^{\alpha-1})$；

$x_\alpha+2^{\alpha-1}\not\equiv-x_\alpha$；$-(x_\alpha+2^{\alpha-1})$

$$\not\equiv x_\alpha \pmod{2^\alpha}$$

又因

$$2^{\alpha-1} \not\equiv 0 \pmod{2^\alpha}$$

$\therefore \quad x_\alpha + 2^{\alpha-1} \not\equiv x_\alpha, \quad -(x_\alpha + 2^{\alpha-1}) \not\equiv -x_\alpha \pmod{2^\alpha}$，

这就证明了条件的充分性。

这个定理的证明过程，实际已给出求同余式（26）的解的过程。

例5·4 解 $x^2 \equiv 57 \pmod{64}$

解 因$57 \equiv 1 \pmod 8$，故有四个解，把

$$x = \pm(1 + 4t_3)$$

代入原同余式，得

$$(1+4t_3)^2 \equiv 57 \pmod{16} \Longrightarrow t_3 \equiv 1 \pmod 2,$$

取 $t_3' = 1$，$t_3 = 1 + 2t_4$，代入（27）得

$$x = \pm(1 + 4(1 + 2t_4)) = \pm(5 + 8t_4),\ t_4 = 0,\ \pm 1,\ \cdots$$

是适合 $x^2 \equiv 57 \pmod{16}$ 的一切整数，再代入原同余式，得

$$(5+8t_4)^2 \equiv 57 \pmod{32} \Longrightarrow t_4 \equiv 0 \pmod 2$$

$\therefore \quad x = \pm(5 + 16t_5)$，$t_5 = 0$，$\pm 1$，$\pm 2$，$\cdots$ 是适合 $x^2 \equiv 57 \pmod{32}$ 的一切整数，同样地

$$(5+16t_5)^2 \equiv 57 \pmod{64} \Longrightarrow t_5 \equiv 1 \pmod 2$$

$\therefore \quad x = \pm(21 + 32t_6)$，$t_6 = 0$，$\pm 1$，$\pm 2$，$\cdots$ 是适合 $x^2 \equiv 57 \pmod{64}$ 的一切整数，即其四解是

$$x \equiv 21,\ -21,\ 53,\ -53 \pmod{64}.$$

从定理5·6，5·7及勒让得符号的性质9°，得

定理5·8 同余式

$$x^2 \equiv a \pmod m,\quad m = 2^\alpha p_1^{\alpha_1} \cdots p_k^{\alpha_k},\quad (a, m) = 1$$

有解的必要条件是：当 $\alpha=2$ 时，$a\equiv1\pmod 4$；
当 $\alpha\geqslant3$ 时，$a\equiv1\pmod 8$，并且 $\left(\frac{a}{p_i}\right)=1, i=1,\cdots,k$。

若上述条件成立，则有解，并且（i）当 $\alpha=0$，1 时解数是 2^k；（ii）当 $\alpha=2$ 时，解数是 2^{k+1}；（iii）当 $\alpha\geqslant3$ 时，解数是 2^{k+2}。

第六节　把奇素数表成二数的平方和

本节主要引用前面的理论来讨论不定方程 $x^2+y^2=p$，$x>0$，$y>0$，p 为奇素数，有解的条件，并进一步讨论不定方程 $x^2+2y^2=p$，$x>0$，$y>0$，p 为奇素数，有解的条件，本节的 p 都代表奇素数。

引理 1. 若 $(k, p)=1$，则勒让得符号之和

$$\sum_{x=0}^{p-1}\left(\frac{x(x+k)}{p}\right)=-1.$$

证明　（i）　若 $(x, p)=1$，则存在 $0<x'<p$ 使得

$$x'x\equiv1\pmod p,$$

并且这样的 x' 是唯一的（定理4·1）。

（ii）　由勒让得符号的性质，及（i）中当 x 过模 p 的互素剩余系时，x' 亦过模 p 的互素剩余系。故得

$$\sum_{x=0}^{p-1}\left(\frac{x(x+k)}{p}\right)=\sum_{x=1}^{p-1}\left(\frac{x(x+k)}{p}\right)=\sum_{x=1}^{p-1}\left(\frac{x'^2x(x+k)}{p}\right)$$

$$=\sum_{x=1}^{p-1}\left(\frac{x'(x+k)}{p}\right)=\sum_{x'=1}^{p-1}\left(\frac{1+kx'}{p}\right)$$

$$=\sum_{x'=0}^{p-1}\left(\frac{1+kx'}{p}\right)-1$$

因为$(k, p)=1$，所以由定理3·5知$1+kx'$（$x'=0, 1, \cdots, p-1$）过模p的完全剩余系，又由定理5·1知

$$\sum_{x'=0}^{p-1}\left(\frac{1+kx'}{p}\right)=0,$$

$$\therefore\quad \sum_{x=0}^{p-1}\left(\frac{x(x+k)}{p}\right)=-1.$$

引理2　设$p=4m+1$为素数，勒让得符号之和

$$S(k)=\sum_{x=0}^{p-1}\left(\frac{x(x^2+k)}{p}\right),$$

当$(k, p)=1$时，则

(i)　$S(k)=2\sum_{x=1}^{2m}\left(\frac{x(x^2+k)}{p}\right)$是偶数；

(ii)　$S(kt^2)=\left(\frac{t}{p}\right)S(k)$.

证明　(i)　由于$p=4m+1$，及勒让得符号的定义与性质，得

$$S(k)=\sum_{x=1}^{p-1}\left(\frac{x(x^2+k)}{p}\right)$$

$$=\sum_{x=1}^{2m}\left(\frac{x(x^2+k)}{p}\right)+\sum_{x=1}^{2m}\left(\frac{(p-x)((p-x)^2+k)}{p}\right).$$

$$\because\quad (p-x)((p-x)^2+k)\equiv -x(x^2+k)\ (\bmod p),$$

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}=(-1)^{2m}=1,$$

$$\therefore \quad S(k)=\sum_{x=1}^{2m}\left[\left(\frac{x(x^2+k)}{p}\right)+\left(\frac{-1}{p}\right)\left(\frac{x(x^2+k)}{p}\right)\right]$$

$$=2\sum_{x=1}^{2m}\left(\frac{x(x^2+k)}{p}\right).$$

（ii） 若 $t\equiv 0\ (\bmod p)$，则$\left(\frac{t}{p}\right)=0$，

$\left(\frac{t}{p}\right)S(k)=0$；

$$S(kt^2)=\sum_{x=0}^{p-1}\left(\frac{x(x^2+kt^2)}{p}\right)=\sum_{x=0}^{p-1}\left(\frac{x}{p}\right)\left(\frac{x^2}{p}\right)$$

$$=\sum_{x=0}^{p-1}\left(\frac{x}{p}\right)=0.$$

$$\therefore \qquad S(kt^2)=\left(\frac{t}{p}\right)S(k).$$

若 $(t,\ p)=1$（即 $t\not\equiv 0\ (\bmod p)$），则 x 与 xt 都是过模 p 的完全剩余系，故

$$S(kt^2)=\sum_{x=0}^{p-1}\left(\frac{x(x^2+kt^2)}{p}\right)=\sum_{x=0}^{p-1}\left(\frac{xt(x^2t^2+kt^2)}{p}\right)$$

$$=\left(\frac{t^3}{p}\right)\sum_{x=0}^{p-1}\left(\frac{x(x^2+k)}{p}\right)=\left(\frac{t}{p}\right)S(k)$$

引理 3 若$\left(\frac{r}{p}\right)=1$，$\left(\frac{n}{p}\right)=-1$，则

$$r\cdot 1^2,\ \cdots,\ r\cdot\left(\frac{p-1}{2}\right)^2;\ n\cdot 1^2,\cdots,n\cdot\left(\frac{p-1}{2}\right)^2 \quad (a)$$

是模 p 的一个互素剩余系。

证明 当 $t=1,2,\cdots,\frac{p-1}{2}$ 之一时，显然，$(rt^2,p)=1$，$(nt^2,p)=1$，并且

$$rt_1^2 \not\equiv rt_2^2,\quad nt_1^2 \not\equiv nt_2^2 \pmod p,\quad 0<t_1<t_2\leqslant\frac{p-1}{2}.$$

因为 n 是模 p 的平方非剩余，r 是模 p 的平方剩余，所以 nt_1^2 亦 p 的平方非剩余，rt_2^2 亦 p 的平方剩余，因而

$$nt_1^2 \not\equiv rt_2^2 \pmod p \left(t_1,\ t_2=1,\ \cdots,\ \frac{p-1}{2}\right)$$

而（a）共有 p－1 个数，所以它是模 p 的一个互素剩余系。

定理5·9 若 p 是形如 4m＋1 的素数，则

$$p=\left(\frac{1}{2}S(r)\right)^2+\left(\frac{1}{2}S(n)\right)^2,$$

其中S(k)是引理 2 中所定义的，即

$$S(r)=\sum_{x=0}^{p-1}\left(\frac{x(x^2+r)}{p}\right),\quad S(n)=\sum_{x=0}^{p-1}\left(\frac{x(x^2+n)}{p}\right);$$

而$\left(\frac{r}{p}\right)=1$，$\left(\frac{n}{p}\right)=-1$。

证明 令 $p-1=2p_1\ (p_1=2m)$，则由引理 2（ii）知道

$$\sum_{t=1}^{p_1}(S(rt^2))^2=\sum_{t=1}^{p_1}\left(\frac{t}{p}\right)^2(S(r))^2=p_1(S(r))^2,$$

$$\sum_{t=1}^{p_1}(S(nt^2))^2=p_1(S(n))^2.$$

又由引理 3，可得

$p_1(S(r))^2+p_1(S(n))^2$

$$=\sum_{t=1}^{p1}(S(rt^2))^2+\sum_{t=1}^{p1}(S(nt^2))^2=\sum_{k=1}^{p-1}(S(k))^2$$

$$=\sum_{k=1}^{p-1}\left[\sum_{x=0}^{p-1}\left(\frac{x(x^2+k)}{p}\right)\right]^2$$

$$=\sum_{k=1}^{p-1}\sum_{y=0}^{p-1}\sum_{x=0}^{p-1}\left(\frac{xy(x^2+k)(y^2+k)}{p}\right)$$

$$=\sum_{x=1}^{p-1}\sum_{y=1}^{p-1}\sum_{k=1}^{p-1}\left(\frac{xy(x^2+k)(y^2+k)}{p}\right).$$

当 $y\neq x$ 且 $y\neq p-x$ 时，$y^2\not\equiv x^2 \pmod p$，此时令 $y^2+k=z$，则

$$(x^2+k)(y^2+k)=z[z+(x^2-y^2)],$$

$$((x^2-y^2),\ p)=1,$$

由引理1，知

$$\sum_{k=1}^{p-1}\left(\frac{xy(x^2+k)(y^2+k)}{p}\right)$$

$$=\left(\frac{xy}{p}\right)\left[\sum_{k=1}^{p-1}\left(\frac{(x^2+k)(y^2+k)}{p}\right)-1\right]$$

$$=\left(\frac{xy}{p}\right)\left[\sum_{z=0}^{p-1}\left(\frac{z[z+(x^2-y^2)]}{p}\right)-1\right]$$

$$=-2\left(\frac{xy}{p}\right).$$

当 $y=x$ 或 $y=p-x$ 时，$y^2\equiv x^2 \pmod p$，则

$$\sum_{k=1}^{p-1}\left(\frac{xy(x^2+k)(y^2+k)}{p}\right)=\left(\frac{xy}{p}\right)\sum_{k=1}^{p-1}\left(\frac{x^2+k}{p}\right)^2$$

$$=(p-2)\left(\frac{xy}{p}\right).$$

事实上，给定了$(x, p)=1$的 x 之后，在1，2，…，$p-1$中有且只有一个值 k，满足 $x^2+k\equiv 0(\bmod p)$。

$\therefore p_1(S(r))^2+p_1(S(n))^2$

$$=\sum_{\substack{x=1 \\ x^2\not\equiv y^2(\bmod p)}}^{p-1}\sum_{y=1}^{p-1}\left[-2\left(\frac{xy}{p}\right)\right]+\sum_{\substack{x=1 \\ x^2\equiv y^2(\bmod p)}}^{p-1}\sum_{y=1}^{p-1}(p-2)\left(\frac{xy}{p}\right)$$

$$=-2\sum_{x=1}^{p-1}\sum_{y=1}^{p-1}\left(\frac{xy}{p}\right)+p\sum_{\substack{x=1 \\ x^2\equiv y^2(\bmod p)}}^{p-1}\sum_{y=1}^{p-1}\left(\frac{xy}{p}\right)$$

$$=-2\left[\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\right]\left[\sum_{y=1}^{p-1}\left(\frac{y}{p}\right)\right]+p\sum_{\substack{x=1 \\ y=x}}^{p-1}\sum_{y=1}^{p-1}\left(\frac{xy}{p}\right)$$

$$+p\sum_{\substack{x=1 \\ y=p-x}}^{p-1}\sum_{y=1}^{p-1}\left(\frac{xy}{p}\right).$$

但 $\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)=0$,

$$\left(\frac{xy}{p}\right)=\begin{cases}\left(\frac{x^2}{p}\right)=1, & \text{当 } y=x \text{ 时;}\\ \left(\frac{-x^2}{p}\right)=1, & \text{当 } y=p-x(p=4m+1) \text{ 时。}\end{cases}$$

$\therefore \quad p_1(S(r))^2+p_1(S(n))^2=2p(p-1)=4pp_1$.

由引理2，知，$\frac{1}{2}S(r)$、$\frac{1}{2}S(n)$都是整数，

$$\therefore \quad p=\left(\frac{1}{2}S(r)\right)^2+\left(\frac{1}{2}S(n)\right)^2.$$

例如，$p=13$，$\left(\frac{1}{13}\right)=1$，$\left(\frac{2}{13}\right)=(-1)^{\frac{13^2-1}{8}}=-1$，

而$\frac{1}{2}S(1)=3$，$\frac{1}{2}S(2)=2$，

$$\therefore \quad 13=3^2+2^2.$$

$p=17$，$17=1^2+4^2$；$p=1289$，$1289=8^2+35^2$。

实际上，我们已经在例1·13中应用连分数的知识证明了定理5·9，但它求"q"的方法，比定理5·9中求$S(r)$，$S(n)$为难。

系 不定方程

$$x^2+y^2=p\ (p\text{是奇素数}) \tag{28}$$

有正整数解的充要条件是：$p=4m+1$。

证明 定理5·9已证明了本系的充分性。

今证其必要性。因为p是奇数，因此如果(28)有解，那末x与y一定一奇一偶，设$x=2k$，$y=2k+1$，则

$$x^2+y^2=4(k^2+h^2+h)+1=4m+1$$

其中$m=k^2+h^2+h$。即p必为$4m+1$形。

定理5·10 不定方程

$$x^2+2y^2=p \tag{29}$$

有正整数解的充要条件是$\left(\frac{-2}{p}\right)=1$，即$p=8m+1$或$p=8m+3$。

证明 (i) 条件的必要性：若(29)有正整数解(x,y)，则

$(y, p)=(y,p)=1$，于是存在整数y'，使得$yy'\equiv 1\ (\bmod p)$，由此得到

$$(x^2+2y^2)y'^2\equiv(xy')^2+2\equiv 0(\bmod p),$$

即$\left(\frac{-2}{p}\right)=1$。

(ii) 条件的充分性：若$\left(\frac{-2}{p}\right)=1$，则$x^2+2\equiv 0(\bmod p)\left(|x|<\frac{p}{2}\right)$，有解．此时

$$0<2+x^2<2+\frac{p^2}{4}<p^2.$$

故存在正整数 m，x，y，使得

$$x^2+2y^2=mp,\ 0<m<p \tag{a}$$

成立〔因若$0<x_0<\frac{p}{2}$是$x^2+2\equiv 0(\bmod p)$的解，则$x_0^2+2=sp(0<s<p)$，此时$y=1$，$x=x_0$，$m=s$〕。设m_0是使(a)成立的最小正整数，下面证明$m_0=1$。

若$m_0>1$，由绝对最小剩余系的性质，立刻知道存在有二整数x_1，y_1使得

$$x\equiv x_1,\ y\equiv y_1(\bmod m_0),\ |x_1|\leqslant\frac{1}{2}m_0,\ |y_1|\leqslant\frac{1}{2}m_0, \tag{b}$$

并且$|x_1|$，$|y_1|$不全为0，否则$x_1=y_1=0\Longrightarrow m_0|x$，$m_0|y\Longrightarrow m_0^2\Big|x^2+2y^2\Longrightarrow m_0^2\Big|m_0p\Longrightarrow m_0|p$，但$m_0<p$，于是$m_0=1$，这与$m_0>1$的假设矛盾。

由(b)，得

$$0<x_1^2+2y_1^2\leqslant\left(\frac{1}{4}+\frac{2}{4}\right)m_0^2<m_0^2,$$

$$x_1^2+2y_1^2\equiv x^2+2y^2=m_0p\equiv 0(\bmod m_0)$$

故 $x_1^2+2y_1^2=m_1m_0$，$0<m_1<m_0$，因此由(a)得

$$m_0^2m_1p=(x^2+2y^2)\left(x_1^2+2y_1^2\right)=(xx_1+2yy_1)^2+ +2(xy_1-x_1y)^2 \quad \text{(c)}$$

又由(b)得

$$\left.\begin{aligned} xx_1+2yy_1\equiv x_1^2+2y_1^2\equiv 0 \pmod{m_0} \\ xy_1-x_1y\equiv x_1y_1-x_1y_1\equiv 0 \pmod{m_0} \end{aligned}\right\} \quad \text{(d)}$$

由(d)及(c)知道，不定方程

$$X^2+2Y^2=m_1p$$

有非负整数解

$$X=\frac{|xx_1+2yy_1|}{m_0},\quad Y=\frac{|xy_1-x_1y|}{m_0},$$

且 $X\neq 0$，$Y\neq 0$。否则，m_1p 是一个数的平方，或一个数平方的二倍，由于 $0<m_1<p$ 及 p 是素数，所以这是不可能的。从而得到，m_1 也是使(a)成立的正整数，这与 m_0 的最小性矛盾，故 $m_0=1$。这就证明了本定理。

例如，$x^2+2y^2=17$ 有解 $x=3$，$y=2$；$x^2+2y^2=13$ 没有正整数解；$x^2+2y^2=43$ 有解 $x=5$，$y=3$。

第七节　四平方和定理与华林问题

前一节讨论了把一个奇素数表成二数平方之和的条件，本节将更一般地讨论一个正整数表成平方和的条件；并证明每一个正整数都可表示成四个整数的平方和(拉格朗日—Lagrange定理)。此外还简单介绍著名的华林(Waring)问题。

任给正整数 n，由算术基本定理知

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k} = n_1^2 n_2, \tag{30}$$

其中 n_2 不含平方因子，因此我们要讨论把正整数表成平方和的问题，关键在于不含平方因数的正整数。

引理1 设 m_1，…，m_s 是 s 个都可表成两个整数平方和的正整数，则 $m_1 m_2 \cdots m_s$ 亦可表成两个整数的平方和。

证明 因为 $m_i = x_i^2 + y_i^2 (i = 1, \cdots, s)$，所以

A） 当 $s = 2$ 时，

$$m_1 m_2 = \left(x_1^2 + y_1^2\right)\left(x_2^2 + y_2^2\right) = (x_1 x_2 + y_1 y_2)^2 + (x_1 y_2 - x_2 y_1)^2.$$

B） 设 $s = k$ 时，结论成立。即

$$m_1 \cdots m_k = \left(x_1^2 + y_1^2\right) \cdots \left(x_k^2 + y_k^2\right) = X'^2 + Y'^2$$

其中 X'，Y' 是整数，则

$$m_1 \cdots m_k m_{k+1} = (X'^2 + Y'^2)\left(x_{k+1}^2 + y_{k+1}^2\right)$$

$$= (X' x_{k+1} + Y' y_{k+1})^2 + (X' y_{k+1} - Y' x_{k+1})^2$$

$$= X^2 + Y^2.$$

引理2 若 s 个正整数 n_1，n_2，…，n_s 都能表成四个整数的平方和，则 $n = n_1 n_2 \cdots n_s$ 亦能表成四个整数的平方和 .

如同引理 1 的证法一样，可用数学归纳法证明之，实际上，只要证当

$$n_1 = x_1^2 + x_2^2 + x_3^2 + x_4^2, \quad n_2 = y_1^2 + y_2^2 + y_3^2 + y_4^2$$

时，$n_1 n_2$ 亦可表成四个整数的平方和，就可以了。而

$$n_1 n_2 = \left(x_1^2 + x_2^2 + x_3^2 + x_4^2\right)\left(y_1^2 + y_2^2 + y_3^2 + y_4^2\right)$$

$$= (x_1 y_1 + x_2 y_2 + x_3 y_3 + x_4 y_4)^2$$

$$+(x_1y_2-y_2x_1+x_3y_4-x_4y_3)^2$$
$$+(x_1y_3-x_3y_1+x_4y_2-x_2y_4)^2$$
$$+(x_1y_4-x_4y_1+x_2y_3-x_3y_2)^2$$
$$=X_1^2+X_2^2+X_3^2+X_4^2.$$

定理5·11 设 $n=n_1^2n_2$，$n>0$且n_2没有平方因数，则n能表成两个整数的平方和的充要条件是：n_2没有形如$4m+3$的因数。

证明 (i) 充分条件：若n_2不含形如$4m+3$的素因数，则n_2的素因数只有2和形如$4m+1$的素数。而$2=1^2+1^2$，又由定理5·9知，n_2的任一奇素因数，都可表成二整数的平方和。由引理1知n_2可表示二整数的平方和。

(ii) 必要条件：若n_2中有一个形如$4m+3$的素因数p，则有一正整数r，使得$p^r|n$。由(30)知n_2不含平方因数，故r是奇数。

如果n能表成两个整数的平方和，即

$$n=x^2+y^2,\ (x,\ y)=d.$$

那末$x=Xd$，$y=Yd$，$(z,\ y)=1$，$n=d^2(X^2+Y^2)$。
因为$p^r|n$且$2\nmid r$，所以$p|X^2+Y^2$且$p\nmid X$，否则，$p|X$，$p|Y\Longrightarrow p|(X,\ Y)$与$(X,\ Y)=1$矛盾.

$$\therefore\quad X^2+Y^2\equiv 0(\mathrm{mod}),\ (p,\ X)=1.$$

由定理4·1知，存在整数X'，使得$XX'\equiv 1(\mathrm{mod}\ p)$，因而

$$(XY')^2\equiv -1(\mathrm{mod}\ p),$$

即$\left(\frac{-1}{p}\right)=1$，但由勒让得符号性质4°知$\left(\frac{-1}{p}\right)$
$=(-1)^{\frac{4m+3-1}{2}}=-1$，从而得到矛盾。

定理5·12 每一个素数，都可表成四个整数的平方和。

证明 $2=1^2+1^2+0^2+0^2$；设p为奇素数分两步来证明，

（i） 证明存在整数x，y，m，使得

$$1+x^2+y^2=mp, \quad 0<m<p. \tag{a}$$

考虑下列 $p+1$ 个整数

$$0^2, 1^2, \cdots, \left(\frac{p-1}{2}\right)^2; -1, -1-1^2, -1-2^2, \cdots, -1-\left(\frac{p-1}{2}\right)^2. \tag{b}$$

因为对模p来说，只有p个不同类的剩余，故(b)中至少有两个关于模p同余。并且 $i \neq j$ 时，$i^2 \not\equiv j^2 \pmod p$，$-1-i^2 \not\equiv -1-j^2 \pmod p$，故存在二整数x，y，使得

$$x^2 \equiv -1-y^2 \pmod p, \quad 0 \leqslant x \leqslant \frac{p-1}{2}, \quad 0 \leqslant y \leqslant \frac{p-1}{2}.$$

因此，$1+x^2+y^2=mp$，而且 $0<1+x^2+y^2<1+2\left(\frac{p}{2}\right)^2<p^2$，故 $0<m<p$。

（ii） 由(i)知道p的一个正倍数mp，能表成四整数的平方和，因此p有一个最小的正倍数 m_0p 能表成四个整数的平方和，则

$$m_0p=x_1^2+x_2^2+x_3^2+x_4^2, \quad 0<m_0<p. \tag{c}$$

今证明 $m_0=1$。

首先，我们证明 m_0 是奇 . 如果 m_0 是偶数，那末 $x_1^2+x_2^2+x_3^2+x_4^2$ 是偶数，此时有且只有下列三种情况之一发生：

（1） x_1，x_2，x_3，x_4 都是偶数；

（2）　x_1，x_2，x_3，x_4都是奇数；

（3）　x_1，x_2，x_3，x_4是两奇两偶；不妨设 x_1，x_2是偶数，x_3，x_4是奇数。

上述情况中，不论那一种都有

$$x_1+x_2,\quad x_1-x_2,\quad x_3+x_4,\quad x_3-x_4$$

都是偶数，因此

$$\frac{1}{2}m_0p=\left(\frac{x_1+x_2}{2}\right)^2+\left(\frac{x_1-x_2}{2}\right)^2+\left(\frac{x_3+x_4}{2}\right)^2+\left(\frac{x_3-x_4}{2}\right)^2$$

即$\frac{1}{2}m_0p$ 能表成四个整数的平方和，这与 m_0的最小性矛盾，故 m_0 是奇数。

其次，假定 $m_0>1$，则 $p>m_0\geqslant 3$，且

$m_0\nmid(x_1,\ x_2,\ x_3,\ x_4)$。因为否则，由(c)得$m_0^2\mid m_0p\Longrightarrow m_0\mid p$，这与$1<m_0<p$矛盾。故存在不全为 0 的四个整数 y_1，y_2，y_3，y_4，使得

$$y_i\equiv x_i\,(\mathrm{mod}\ m_0),\quad |y_i|<\frac{1}{2}m_0,\quad i=1,2,3,4 \tag{d}$$

因此$0<y_1^2+y_2^2+y_3^2+y_4^2<4\left(\frac{1}{2}m_0\right)^2=m_0^2$，由(d)及（c）得

$$y_1^2+y_2^2+y_3^2+y_4^2\equiv x_1^2+x_2^2+x_3^2+x_4^2\equiv 0(\mathrm{mod}\ m_0),$$

$$\therefore\qquad y_1^2+y_2^2+y_3^2+y_4^2=m_0m_1,\quad 0<m_1<m_0, \tag{e}$$

由引理 2 及(c)，(e)得到

$$m_0^2m_1p=\left(x_1^2+x_2^2+x_3^2+x_4^2\right)\left(y_1^2+y_2^2+y_3^2+y_4^2\right)$$

$$= z_1^2 + z_2^2 + z_3^2 + z_4^2 \quad \text{(f)}$$

其中 z_1, z_2, z_3, z_4 都是引理 2 中形如 X_1, X_2, X_3, X_4 的整数。再由(c)及(d)知道

$$z_1 = X_1 = \sum_{i=1}^{4} x_i y_i = \sum_{i=1}^{4} x_i^2 \equiv 0 \pmod{m_0};$$

$$z_2 = X_2 = x_1 y_2 - x_2 y_1 + x_3 y_4 - x_4 y_3 \equiv x_1 x_2 - x_2 x_1 + x_3 x_4 - x_4 x_3 \equiv 0 \pmod{m_0}$$

同理，$z_3 \equiv 0 \pmod{m_0}$，$z_4 \equiv 0 \pmod{m_0}$。

$$\therefore \quad z_i = m_0 t_i \ (i = 1, 2, 3, 4),$$

代入(f)得

$$m_1 p = t_1^2 + t_2^2 + t_3^2 + t_4^2,$$

这与 m_0 的最小性矛盾，所以 $m_0 = 1$。定理获证。

由引理 2，定理 5·12 及 $1 = 1^2 + 0^2 + 0^2 + 0^2$，即得

定理5·13 （拉格朗日—Lagrange—定理）每一个正整数都能表成四个整数的平方和。

拉格朗日定理，仅解决了所谓的华林（Waring)问题的一个特例（猜测的第一部分）。

华林在1770年提出一个猜测："每一个正整数都是 4 个整数的平方和；9 个正整数的立方和；19个整数的四方和等等。"言下之意，他认为下列结论是正确的：

对于一个给定的正整数 k，存在一个正整数 $S = S(k)$，使得每一个正整数 n，都能表成 S 个非负整数的 k 方和。

一般认为，这个猜测是正确的。

例如，$k = 2$ 时，$S = S(2) = 4$；$k = 3$ 时，$S = S(3) = 9$；$k = 4$ 时，$S = S(4) = 19$ 等等。

但是华林自己并没有证明这个结论。而这个结论就是堆垒数论中著名的华林问题。首先解决华林问题的是希尔伯特（Hilbert），他在1909年证明了对于每一个 k，都可以找到 $S=S(k)$，使每一个正整数都能表成 S 个非负整数的 k 方和。

进一步我们要问究竟最小的 S 是什么？通常用 $g(k)$ 表示最小的 S。于是最好能证明，每一个正整数都可表成 $g(k)$ 个非负整数的 k 方和。即任给 $n(>0)$ 下之不定方程常有解：

$$n=x_1^k+x_2^k+\cdots+x_s^k\ (x_i\geqslant 0,\ i=1,2\cdots,S) \quad (31)$$

由拉格朗日定理，知道 $g(2)\leqslant 4$，另一方面可以验证，$7=2^2+3\times 1^2$ 不能用三个平方和去表示，故 $g(2)=4$。可以证明 $g(3)=9$，也可以证明充分大的正整数可以表成7个非负整数的立方和，后者当然比前者更有意义。因此，我们用 $G(k)$ 代表对于充分大的正整数能表成 S 个 k 方和的 S 的最小值。已经证明了 $G(2)=4$，$G(3)\geqslant 4$ 及 $G(3)\leqslant 7$（林尼克，Линник），$G(4)=16$（德汶颇特，Devenport），对于其他的 $G(k)$ 还没有最后的结果。

继希尔伯特之后，首先由哈代（Hardy）及李特伍德（Littlewood）证明了

$$G(k)\leqslant(1+\varepsilon(k))k2^{k-2}, \quad (32)$$

其中 $\varepsilon(k)\to 0$，当 $k\to\infty$ 时。并猜测：当 $k=2^m$，$m>1$ 时，$G(k)=4k$；而 $k\neq 2^m$，$m>1$ 时，$G(k)\leqslant 2k+1$。至今，除 $k=2$，4以外，还未断定这个猜测是否正确。

苏联维诺格拉朵夫（И·М·Виноградов）大大改进了(32)，他先证明了

$$G(k)<6k\ln k+(4+\ln 216)k; \quad (33)$$

后来又证明了

$$G(k)<k(3\ln k+11). \quad (34)$$

运用他的方法，狄克逊（Dickson），皮拉（Pillai），奈文（Niven）证明了，当 $k\geqslant 6$，及$3^k-2^k+2\leqslant(2^k-1)\left[\left(\frac{3}{2}\right)^k\right]$成立时，

$$g(k)=2^k+\left[\left(\frac{3}{2}\right)^k\right]-2. ^* \quad (34)$$

应该指出，我国数学家华罗庚在研究华林问题中用 s 个 k 方和表 n 的表法数目的渐近公式方面，得到了比哈代与李特伍德更好的结果。华罗庚在等幂和的问题方面还得到以下结果：设M(k)表示能使下列不定方程组有解的 s 的最小值：

$$\begin{cases} x_1^h+\cdots+x_s^h=y_1^h+\cdots+y_s^h(h=1,\ 2,\ \cdots,\ k), \\ x_1^{k+1}+\cdots+x_s^{k+1}\neq y_1^{k+1}+\cdots+y_s^{k+1}. \end{cases} \quad (35)$$

$$M(k)\leqslant(k+1)\left(\left[\frac{\ln\frac{1}{2}(k+2)}{\ln\left(1+\frac{1}{k}\right)}\right]+1\right)\sim k^2\ln k, \quad (36)$$

其中“～”表示“相当”：即$f(x)\sim g(x)\Longleftrightarrow\lim\limits_{x\to\infty}\frac{f(x)}{g(x)}=1$。

这个结果至今还是最好的。他又在1952年，证明 $S>S_0$（其中 S_0是 k 的一个函数 $S_0\sim 3k^2\ln k$）时，可以得到(35)解数的近似公式。

---

* 三氏是在 g(k)的下限 $g(k)\geqslant 2^k+\left[\left(\frac{3}{2}\right)^k\right]-2$的基础上，经过维诺格拉朵夫方法的实际计算得到(34)的结论。至今除$k=4$外，其他 g(k) 都已求出。

关于华林问题之研究，初等方法一般并不能得到最好的结果。今仅举几例于下：

定理5·13 $g(4)\leqslant 50$

证明 由定理5·12知，任一正整数N，有

$$N=a^2+b^2+c^2+d^2.$$

今研究恒等式

$$\begin{aligned}6N^2&=6(a^2+b^2+c^2+d^2)^2\\&=(a+b)^4+(a-b)^4+(c+d)^4+(c-d)^4\\&\quad+(a+c)^4+(a-c)^4+(b+d)^4+(b-d)^4\\&\quad+(a+d)^4+(a-d)^4+(b+c)^4\\&\quad+(b-c)^4.\end{aligned}\tag{37}$$

任一整数 n可以表为

$$n=6N+r,\ (r=0,\ 1,\ \cdots,\ 5之一),$$

$$\therefore\qquad n=6\left(x_1^2+x_2^2+x_3^2+x_4^2\right)+r$$

由(37)知，$6x_1^2$、$6x_2^2$、$6x_3^2$、$6x_4^2$都可表为12个整数的四次方之和。故 n是$4\times 12+5=53$个四次方之和。

其次，因为$81\equiv 3$，$16\equiv 4$，$17\equiv 5 \pmod 6$，故，若$n\geqslant 81$，则可表为

$$n=6N+t,\ (N\geqslant 0,\ t=0,\ 1,\ 2,\ 81,\ 16,\ 17之一),$$

而

$$1=1^4,\ 2=1^4+1^4,\ 81=3^4,\ 16=2^4,\ 17=2^4+1^4.$$

故同上法，若 $n\geqslant 81$，则可表为$4\times 12+2=50$个四次之和。

当 $n\leqslant 80$时，容易算出：若 $n\leqslant 50$时，则$n=n\cdot 1^4$，若$50<n\leqslant 80$时，则 $n=3\times 2^4+(n-48)\cdot 1^4$，它是 $3+n-48<50$个四方数之和。

综合上述，得

$$g(4)\leqslant 50.$$

系 $g(8)\leqslant 42273$.

证明 由恒等式

$$5040(a^2+b^2+c^2+d^2)^4=6\sum(2a)^8+60\sum(a\pm b)^8+\sum(2a\pm b\pm c)^8+6\sum(a\pm b\pm c\pm d)^8, \tag{38}$$

知，(38)的右边共有840(=6×4+60×12+4×3×4+6×4×2)*个8次方。与定理5·13的证法一样，对任一正整数 n，都有

$$n=5040N+r,\ 0\leqslant r\leqslant 5039.$$

由定理5·13及定理5·12知道N可表为 $g(4)(\leqslant 50)$ 个非负整数的4方和，且和的每项都可表成 $a^2+b^2+c^2+d^2$ 形的和。又因 $r\leqslant 5039$ 时，都可表成 $\leqslant 273$ 个1及2的8次方之和。故得

$$g(8)\leqslant 840\,g(4)+273\leqslant 42273.$$

定理5·14 $G(3)\leqslant 13$

证明 由恒等式

$$\sum_{i=1}^{4}((z^3+x_i)^3+(z^3-x_i)^3)=8z^9+6z^3\left(x_1^2+x_2^2+x_3^2+x_4^2\right) \tag{39}$$

知，若一数可以表成

$$8z^9+6mz^3,\ 0\leqslant m\leqslant z^6. \tag{40}$$

则此数一定可以表为8个立方数的和。

由定理5·12知 $m=x_1^2+x_2^2+x_3^2+x_4^2$，且 $x_i\leqslant z^3$。

---

* 这是(38)右边各项所含8次方的项数，其中第一至三项中的"Σ"都表示a，b，c，d的各种可能出现的情况，而第四项的"Σ"表示取"+"号时，后三数同取正号，取"－"号时后三数同取负号。

令 z 是6除余1的正整数（即 $z\equiv 1(\bmod 6)$ 且 $z>0$）. I_z 表示隔间

$$\phi(z)=11z^9+(z^3+1)^3+125z^3\leqslant n\leqslant 14z^9=\psi(z). \quad (41)$$

显然当 z 充分大时，有

$$\phi(z+6)<\psi(z). \quad (42)$$

即 I_z 都是互相衔接的隔间. 即当 n 充分大时，必有一 z 使(41)成立.

由下式定义 r，S 及 N：

$$n\equiv 6r(\bmod z^3),\ 1\leqslant r\leqslant z^3;$$

$$n\equiv S+4(\bmod 6),\ 0\leqslant S\leqslant 5;$$

$$N=(r+1)^3+(r-1)^3+2(z^3-r)^3+(Sz)^3.$$

由此可得

$$0<N<(z^3+1)^3+3z^9+125z^3=\phi(z)-8z^9\leqslant n-8z^9$$

$$\therefore \quad 8z^9<n-N<14z^9. \quad (43)$$

现在证明，$n-N$ 可以表为(40)的形式.

$$n-N\equiv 6r-(r+1)^3-(r-1)^3+2r^3\equiv 0\equiv 8z^9(\bmod z^3)$$

又因 $x^3\equiv x(\bmod 6)$ 对于任意整数 x 都成立，故有

$$n-N\equiv S+4-(r+1)-(r-1)-2(z^3-r)-Sz$$

$$\equiv S+4-z(S+2)\equiv 2\equiv 8\equiv 8z^9(\bmod 6),$$

所以 $n-N-8z^9$ 是 $6z^3$ 的倍数，即

$$n=N+8z^9+6mz^3.$$

由(43)及上式即得 $0\leqslant m\leqslant z^6$.

上面证明了，对充分大的整数 n，$n-N$ 可以表成八个非负整数的立方和，由 N 的定义知，N 可表成5个非负整数的立方和.

$$\therefore \quad G(3)\leqslant 13.$$

定理5·15 $g(3)\leqslant 13$

证明 先算出若$z\geqslant 373$，则$\phi(z+6)\leqslant\psi(z)$，或者当$t\geqslant 379$时

$$11t^9+(t^3+1)^3+125t^3\leqslant 14(t-6)^9,$$

即
$$14\left(1-\frac{6}{t}\right)^9\geqslant 12+\frac{3}{t^3}+\frac{128}{t^6}+\frac{1}{t^9} \tag{44}$$

由于当$0<\delta<1$时，$(1-\delta)^m\geqslant 1-m\delta$，故

$$\left(1-\frac{6}{t}\right)^9\geqslant 1-\frac{54}{t}.$$

所以若能证明

$$14\left(1-\frac{54}{t}\right)\geqslant 12+\frac{3}{t^3}+\frac{128}{t^6}+\frac{1}{t^9},$$

或
$$2(t-7\times 54)\geqslant\frac{3}{t^2}+\frac{128}{t^5}+\frac{1}{t^8}$$

成立，则(44)成立。由于$t\geqslant 7\times 54+1=379$，故(44)成立。

所以当$z\geqslant 373$时，由(41)知诸隔间I_z是衔接的。即当

$$n\geqslant 14\times(373)^9$$

时必落在一个隔间I_z中。又$10^{25}>14\times(373)^9$故任一整数$n\geqslant 10^{25}$时，一定可以表成13个非负整数的立方和。

其次，证明不大于10^{25}的数也是十三个立方数的和。

先造表可知，小于40000的数，除23及239是九个立方数之和外，其余都是8个立方数的和。也就是说，若$240\leqslant n\leqslant 40000$，则$n$是八个立方数之和。

若$N\geqslant 1$及$m=[N^{\frac{1}{3}}]$，则

$$N-m^3=(N^{\frac{1}{3}})^3-m^3\leqslant 3N^{\frac{2}{3}}(N^{\frac{1}{3}}-m)<3N^{\frac{2}{3}}.$$

令$n=240+N$，$240\leqslant n\leqslant 10^{25}$，即$0\leqslant N<10^{25}$，

则

$$N=m^3+N_1,\quad m=[N^{\frac{1}{3}}],0<N_1<3N^{\frac{2}{3}},$$

$$N_1 = m_1^3 + N_2,\quad m_1 = [N_1^{\frac{1}{3}}],\quad 0 < N_2 < 3N_1^{\frac{2}{3}},$$

$$\cdots\quad \cdots\quad \cdots\quad \cdots\quad \cdots\quad \cdots,$$

$$N_4 = m_4^3 + N_5,\quad m_4 = [N_4^{\frac{1}{3}}],\quad 0 < N_5 < 3N_4^{\frac{2}{3}}.$$

$$\therefore\quad n = 240 + N = 240 + N_5 + m^3 + m_1^3 + m_2^3 + m_3^3 + m_4^3.$$

由于

$$0 < N_5 \leqslant 3N_4^{\frac{2}{3}} \leqslant 3(3N_3^{\frac{2}{3}})^{\frac{2}{3}} \leqslant \cdots$$

$$\leqslant 3^{1+\frac{2}{3}+(\frac{2}{3})^2+(\frac{2}{3})^3+(\frac{2}{3})^4} N^{(\frac{2}{3})^5}$$

$$= 27\left(\frac{N}{27}\right)^{(\frac{2}{3})^5} < 27\left(\frac{10^{25}}{27}\right)^{(\frac{2}{3})^5} < 35000$$

$$\therefore\quad 240 \leqslant 240 + N_5 < 35240 < 40000.$$

即$240 + N_5$可以表成八个立方数之和。故$n = 240 + N$可以表成13个立方数之和。

$$\therefore\quad g(3) \leqslant 13.$$

注意：$3^{1+\frac{2}{3}+\cdots+(\frac{2}{3})^4} N^{(\frac{2}{3})^5} = 3^{3(1-(\frac{2}{3})^5)} N^{(\frac{2}{3})^5}$

$$= \frac{27}{3^{3(\frac{2}{3})^5}} \cdot N^{(\frac{2}{3})^5} = 27\left(\frac{N}{27}\right)^{(\frac{2}{3})^5}.$$

由恒等式

$$60(a^2 + b^2 + c^2 + d^2)^3 = \sum(a \pm b \pm c)^6 + 2\sum(a \pm b)^6 + 36\sum a^6,$$

可以证明

系 $g(6) \leqslant 184g(3) + 59 \leqslant 2451.$

习　　题

1．证明，同余式 $x^2+1\equiv 0 \pmod p$，$p=4m+1$为素数的解是：

$$x\equiv \pm(2m)! \pmod p$$

2．写出与同余式

$$8x^4-9x^3+12x^2-8\equiv 0 \pmod{72} \qquad (a)$$

等价的以素数乘方为模的同余式组

3．二次同余式

$$ax^2+bx+c\equiv 0 \pmod m,\ (a>0) \qquad (\alpha)$$

都可以化成

$$y^2\equiv D \pmod{4am}, \qquad (\beta)$$

其中$D=b^2-4ac$，$y=2ax+b$。

所谓“化成”的意义是：(α)的每一个解都可以从(β)的某一个解导出。

4．将下列二次同余式化成上题(β)的形式：

(i)　$4x^2-11x-3\equiv 0 \pmod{13}$；

(ii)　$5x^2-17x+16\equiv 0 \pmod{45}$；

(iii)　$12x^2+8x-15\equiv 0 \pmod{44}$。

5．求出模37的平方剩余和平方非剩余。

6．证明，模 p 的两个平方剩余之积，两个平方非剩余之积，都是平方剩余。一个平方剩余和一个平方非剩余之积是平方非剩余(欧拉定理)。

7．用欧拉判别法确定5，7，8中哪些是模17的平方非剩余？

8．以 $p=19$，$a=5$为例来验证勒让得符号的性质7°。

9．当 α 是大于 1 的整数时，若同余式

$$x^2\equiv a \pmod{p^\alpha}$$

有解，则其解为 $x\equiv \pm uv \pmod{p^2}$。其中v、u 是满足：当 $b^2\equiv a \pmod p$时，

$$(b-\sqrt{a})^2=t-v\sqrt{a},\quad tu\equiv a \pmod{p^2}.$$

10. 用上题方法，解下列同余式：

(i) $x^2 \equiv 7 \pmod{27}$； (ii) $x^2 \equiv 39 \pmod{625}$.

11. 计算勒让得符号：

(i) $\left(\frac{94}{109}\right)$； (ii) $\left(\frac{111}{271}\right)$； (iii) $\left(\frac{342}{677}\right)$；

(iv) $\left(\frac{93}{131}\right)$； (v) $\left(\frac{2115}{6269}\right)$； (vi) $\left(\frac{589}{1283}\right)$.

其中诸“分母”都是素数。

12. 计算勒让得符号及雅可比符号：

(i) $\left(\frac{47}{125}\right)$； (ii) $\left(\frac{5610}{6649}\right)$； (iii) $\left(\frac{131}{283}\right)$；

(iv) $\left(\frac{116}{397}\right)$； (v) $\left(\frac{328}{625}\right)$.

13. 直接计算雅可比符号$\left(\frac{521}{825}\right)$，然后通过分解成勒让得符号来计算，并验证其结果。

14. 判别下列同余式是否有解：

(i) $x^2 \equiv 429 \pmod{563}$；

(ii) $x^2 \equiv 680 \pmod{769}$；

(iii) $x^2 \equiv 503 \pmod{1013}$.

其中503，563，769，1013都是素数。

15. 求出以-2为平方剩余的素数的一般表达式，以-2为平方非剩余的素数的一般表达式。

16. 设 n 是正整数，$8n+7$是素数，证明

$$2^{4n+3} \equiv 1 \pmod{8n+7}.$$

并由此证明

$$23 \mid 2^{11}-1,\ 47 \mid 2^{23}-1,\ 503 \mid 2^{251}-1.$$

17. 求以± 3为平方剩余的素数的一般表达式，什么素数以± 3为平方非剩余？

18. 求以 3 为最小平方非剩余的素数的一般表达式。

19. 证明：当$p=4k+1$时，二数 a 与 $p-a$ 同为平方剩余，或

同为平方非剩余；而当 $p=4k+3$ 时，二数 a 与 $p-a$ 中一个是平方剩余，而另一个是平方非剩余。

20．证明：x^2-a 的素约数，一定是 t^2-au^2 的约数；反之，当 $(t, u)=1$ 时，x^2-a 与 t^2-au^2 有相同的素约数。

21．当 $(t, u)=1$ 时，求形如 (i) t^2-3u^2；(ii) t^2+7u^2；(iii) t^2-7u^2；(iv) t^2-14u^2；(v) t^2-5u^2 的一切素约数。

22．用柯尔金法解同余式：

(i) $x^2\equiv 11 \pmod{313}$；(ii) $x^2\equiv 8 \pmod{641}$。

23．用第 9 题的方法，解同余式：

(i) $x^2\equiv 24 \pmod{125}$；(ii) $x^2\equiv 18 \pmod{343}$；

(iii) $x^2\equiv 13 \pmod{243}$。

24．应用定理5·7，解同余式：

(i) $x^2\equiv 57 \pmod{512}$；(ii) $x^2\equiv 41 \pmod{1024}$；

(iii) $x^2\equiv 17 \pmod{16384}$。

25．证明对于任意素数 p（包括 $p=2$），同余式

$$x^2\equiv 0 \pmod{p^\alpha}$$

有 $p^{\left[\frac{\alpha}{2}\right]}$ 个不同解。

26．解同余式：

(i) $x^2\equiv 0 \pmod{625}$；(ii) $x^2\equiv 0 \pmod{1331}$。

27．解同余式：

(i) $x^2\equiv 34 \pmod{495}$；(ii) $x^2\equiv 48 \pmod{416}$。

28．解同余式：

(i) $8x^2+15x-6\equiv 0 \pmod{56}$；

(ii) $12x^2-11x-1\equiv 0 \pmod{30}$

29．证明，不定方程

$$x^2+3y^2=p \qquad \text{(a)}$$

有正整数解的充要条件是 $\left(\frac{-3}{p}\right)=1$。

30．证明：$G(2)=4$。

第六章　原根与指数

第五章中讨论了同余式

$$x^2 \equiv a \pmod{m}$$

有解的条件及其解法，并把模为形如 $8k+1$ 的素数 p 的一般解法留于本章来讨论。

本章将进一步讨论同余式

$$x^n \equiv a \pmod{m} \qquad (1)$$

有解的条件。为此引入在数论中很有用的原根和指数的概念，并通过对它们性质的研究，把(1)式对某些特殊的 m 有有解的条件用指数表达出来，最后解决前章所遗留的问题。并附带介绍在数论中具有重要地位的特征函数的概念。

第一节　原　根

本节主要讲清，模 m 为什么数时，m 的原根存在。为此，首先要引入 a 对于模 m 所属方次数的概念及其性质。

由欧拉定理知道，若 $(a, m)=1$，$m>1$，则 $a^{\varphi(m)} \equiv 1 \pmod{m}$。所以

$\forall a, (a, m)=1 \Longrightarrow \exists$ 正整数 $\delta \ni a^\delta \equiv 1 \pmod{m}$。因此，亦存在一个最小的正整数 δ，使得

$$a^\delta \equiv 1 \pmod{m}.$$

定义6·1　若 $m>1$，$(a, m)=1$，则使同余式

$$a^\delta \equiv 1 \pmod{m}$$

成立的最小正整数 δ 叫做 a 对于模 m 所属的方次数（the order to which a belonge to modulus m），或简称为

a 对模 m 属于 δ (a belonge to δ to modulus m). 记作

$$a\in_m\delta.$$

若 a 对模 m 属于 $\varphi(m)$，即 $a\in_m\varphi(m)$，则 a 叫做模m 的一个原根 (primitive root).

例如，$2\in_7 3$，$2\in_{11}10$，$\varphi(11)=10$，$\varphi(7)=6$，故 2 是模11的原根，但不是模 7 的原根。

5 是模 3，模 6，模 9，模18的原根. 如，因为 $\varphi(9)=6$，而

$$5^2\equiv 7,\quad 5^3\equiv -1,\quad 5^4\equiv 4,\quad 5^5\equiv 2,$$

$5^6\equiv 1\ (\mathrm{mod}\ 9)$.

关于模 m的原根的存在和数量问题，留在本节后面及下一节来讨论，现在先研究a对模m所属方次数δ的基本性质。

定理6·1 若 $a\in_m\delta$，则 $1=a^0$，a，a^2，…，$a^{\delta-1}$ 对模 m 是两两互不同余的。

证明 用反证法证明之. $(a, m)=1$，若存在二整数k，l，$0\leqslant k<l<\delta$，使得

$a^k\equiv a^l\ (\mathrm{mod}\ m)\Longrightarrow a^{l-k}\equiv 1\ (\mathrm{mod}\ m)$ 这与 δ 的 最小性矛盾.

定理6·2 若 $a\in_m\delta$，则 $a^\gamma\equiv a^{\gamma'}(\mathrm{mod}\ m)$成立的充要条件是$\gamma\equiv\gamma'(\mathrm{mod}\ \delta)$。特别是 $a^r\equiv 1\ (\mathrm{mod}\ m)$ 成立的充要条件是：$\delta|\gamma$。

证明 由带余除法得

$$\begin{cases}\gamma=\delta q+r, & 0\leqslant r<\delta;\\ \gamma'=\delta q'+r', & 0\leqslant r'<\delta.\end{cases}\qquad(\alpha)$$

$\because\quad a^\delta\equiv 1\ (\mathrm{mod}\ m)$,

$$\therefore\quad\begin{cases}a^\gamma=(a^\delta)^q\cdot a^r\equiv a^r(\mathrm{mod}\ m),\\ a^{\gamma'}=(a^\delta)^{q'}\cdot a^{\gamma'}\equiv a^{\gamma'}(\mathrm{mod}\ m).\end{cases}\qquad(\beta)$$

因此，$a^{\gamma}\equiv a^{\gamma'}(\mathrm{mod}\ m)$的充要条件是：$a^{\gamma}\equiv a^{\gamma'}(\mathrm{mod}\ m)$。由定理6·1及$0\leqslant r<\delta$，$0\leqslant r'<\delta$，即知：若$a^{r}\equiv a^{\gamma'}(\mathrm{mod}\ m)$，则$r=r'$；反之，若$r=r'$，则$a^{r}\equiv a^{\gamma'}(\mathrm{mod} m)$。故$a^{\gamma}\equiv a^{\gamma'}(\mathrm{mod}\ m)$的充要条件是$r=\gamma'$，即$r\equiv\gamma'(\mathrm{mod}\delta)$。

特别当$\gamma'=0$时，$a^{\gamma}\equiv 1\ (\mathrm{mod}\ m)$成立的充要条件是$\delta|r$（(α)第一式中$r=0$）。

在定理6·2中，取$\gamma'=0$，$\gamma=\varphi(m)$，由欧拉定理得

系 1 若$a\in_{m}\delta$，则$\delta|\varphi(m)$。

系 2 设$0<a<b$，$(a,\ b)=1$，$b=2^{\alpha}5^{\beta}b_1$，$(b_1,\ 10)=1$，$b_1\neq 1$。若将有理数$\frac{a}{b}$化成循环节长为δ的循环小数时，则$\delta|\varphi(b_1)$。

证明 由定理3·8及系的证明中知道$\frac{a}{b}$化成循环小数的循环节的长度t，是使

$$10^{t}\equiv 1\ (\mathrm{mod}\ b_1)$$

成立的最小正整数$\delta(=t)$，这就是说，该循环节的长度就是10对模b_1所属的方次数，故由系1知，$\delta|\varphi(b_1)$。

定理6·3 若$x\in_{m}ab$，$a>0$，$b>0$，则$x^{a}\in_{m}b$。

证明 因为$(x,\ m)=1\Longrightarrow(x^{a},\ m)=1$，所以$x^{a}$对模m的所属方次数是存在的。设$x^{a}$对模m属于$\delta$，则$x^{a\delta}\equiv 1\ (\mathrm{mod}\ m)$。由定理6·2知，$ab|a\delta\Longrightarrow b|\delta$。

另一方面，因为$x\in_{m}ab$，所以$(x^{a})^{b}\equiv 1\ (\mathrm{mod}\ m)$，而$x^{a}\in_{m}\delta$，故由定理6·2知$\delta|b$，又因b和$\delta$都是正整数，

$\therefore\qquad b=\delta$。

定理6·4 若$x\in_{m}a$，$y\in_{m}b$，并且$(a,\ b)=1$，则$xy\in_{m}ab$。

证明 因为$(x,\ m)=(y,\ m)=1\Longrightarrow(x\,y,\ m)=1$

$\Longrightarrow \exists \delta \ni xy \in_m \delta$。设

$xy \in_m \delta \Longrightarrow (xy)^\delta \equiv 1 \pmod{m} \Longrightarrow 1 \equiv (xy)^{b\delta} \equiv$
$\equiv x^{b\delta} y^{b\delta} \equiv x^{b\delta} \pmod{m} \Longrightarrow a \mid b\delta$，又因

$(a, b) = 1 \Longrightarrow a \mid \delta$。

同理可证，$b \mid \delta$，而$(a, b) = 1$，故

$$ab \mid \delta.$$

另一方面，

$(xy)^{ab} = (x^a)^b (y^b)^a \equiv 1 \pmod{m} \Longrightarrow \delta \mid ab$。

由于 $ab > 0$，$\delta > 0$，

$\therefore \qquad \delta = ab$。

例如，$3 \in_{13} 3$，$5 \in_{13} 4$，$(3, 5) = 1 \Longrightarrow 3 \times 5 \in_m 3 \times 4 \Longrightarrow 2 \in_{13} 12 \Longrightarrow 2$ 是模13的原根。

本节下面将讨论原根的存在条件。

并非对于任何正整数 m 为模的原根都存在，实际上，当且仅当 $m = 2$，4，p^α，$2p^\alpha$（p 为奇素数，α 为正整数）时，m 的原根才存在，这就是本节要证明的主要结论。

先讨论 $m = p$ 为奇素数的情况，本章下面各节 p 都代表奇素数。

定理6·5 模 p 的原根是存在的。

证明 在模 p 的互素剩余系 1，2，…，$p-1$ 中每一个数都有它自己所属的方次数，把这 $p-1$ 个数所属的不同的方次数，记作

$$\delta_1, \delta_2, \cdots, \delta_r \tag{a}$$

令

$$\tau = [\delta_1, \delta_2, \cdots, \delta_r] = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_k^{\alpha_k} \tag{b}$$

是 τ 的标准分解式。

(i) 证明，$\exists g \ni g \in_m \tau$。事实上，在(b)里 $q_s^{\alpha_s}$ $(s = 1$，

2，…，k)一定整除(a)中的某一δ_i，即$\delta_i = tq_s^{\alpha_s}$，若$x_s \in_p \delta_i, x_s = x^t$，则由定理6·3，有$x^t \in_p q_s^{\alpha_s}$。因此在1，2，…p－1中存在k个数$x_1, x_2, \cdots, x_k$，使得$x_s \in_p q_s^{\alpha_s}$（s＝1，…，k）。因为$q_1, q_2, \cdots, q_k$两两互素，由定理6·4知道，$g = x_1 \cdots x_k$对模p属于τ。

(ii) 今证明$\tau = p-1$，这样g就是模p的原根了。

因为$\delta_s | \tau (s=1, 2, \cdots, r)$，而且1，2，…，p－1中任何数所属的方次数，都在(a)中出现。所以

$$x^\tau \equiv 1 \pmod p$$

有p－1个解$x \equiv 1, 2, \cdots, p-1 \pmod p$，由定理4·11系2知道$\tau \geqslant p-1$；又由定理6·2系1知，$\delta_s | p-1 (s=1, 2, \cdots, r)$，故$\tau | p-1$。

$\therefore \quad \tau = p-1, \ g \in_p \varphi(p)$。

定理6·6 设g是模p的一个原根，则存在一个整数t_0，使得由等式$(g+pt_0)^{p-1} = 1 + pu_0$所确定的$u_0$不能被p整除，并且对应这个$t_0$的$g+pt_0$就是模$p^\alpha$的元根，其中α是大于1的任何整数。

证明 ∵ $g^{p-1} \equiv 1 \pmod p \Longrightarrow \exists$整数$T_0 \ni$

$$g^{p-1} = 1 + pT_0.$$

对于任何整数t，

$$(g+pt)^{p-1} = g^{p-1} + (p-1)ptg^{p-2} + \cdots + (pt)^{p-1}$$
$$= 1 + p(T_0 - g^{p-2}t + pT) = 1 + pu \quad (a)$$

其中$u = T_0 - g^{p-2}t + pT$，T是t的整系数多项式，显然对任何整数来说，

$$u \equiv T_0 - g^{p-2}t \pmod p, \ (g^{p-2}, p) = 1.$$

同余式

$$g^{p-2}t - T_0 \equiv 0 \pmod p$$

只有一个解，故存在 t_0，使得 $g^{p-2}t_0 - T \not\equiv 0 \pmod p$，$t_0$ 所对应的 $u_0 = T_0 - g^{p-2}t_0 + pT$（$T$ 中的 t 以 t_0 代替）不被 p 所整除。

应用具有上述特点的 t_0，得

$$(g + pt_0)^{p(p-1)} = (1 + pu_0)^p = 1 + p^2u_1, \qquad \text{(b)}$$

其中 $u_1 = u_0 + C_p^2 u_0{}^2 + C_p^3 pu_0{}^3 + \cdots + p^{p-2}u_0^p \equiv u_0 \pmod p$，因而 $p \nmid u_1$，同样可得

$$(g + pt_0)^{p^2(p-1)} = (1 + p^2u_1)^p = 1 + p^3u_2,$$
$$(g + pt_0)^{p^3(p-1)} = (1 + p^3u_2)^p = 1 + p^4u_3, \qquad \text{(c)}$$
$$\cdots \quad \cdots \quad \cdots$$

其中 $u_0 \equiv u_1 \equiv u_2 \equiv u_3 \equiv \cdots \pmod p$，即 $p \nmid u_s (s = 0, 1, 2, 3, \cdots)$。设 $g + pt_0 \in {}_{p^\alpha}\delta$，则

$$(g + pt_0)^\delta \equiv 1 \pmod{p^\alpha} \qquad \text{(d)}$$
$$\Longrightarrow (g + pt_0)^\delta \equiv 1 \pmod p.$$

而 $g + pt_0 \equiv g \pmod p$ 是模 p 的一个原根，故 $p - 1 \mid \delta$。另一方面，由定理6·2的系1知 $\delta \mid \varphi(p^\alpha)$，即 $\delta \mid p^{\alpha-1}(p-1)$，故 $\delta = p^{r-1}(p-1)$，r 是 $1, 2, \cdots, \alpha$ 中的一个数。把此结果代入(d)式，然后再由(b)，(c)及(d)得，

$$1 + p^r u_{r-1} \equiv 1 \pmod{p^\alpha} \Longrightarrow p^r u_{r-1} \equiv 0 \pmod{p^\alpha},$$

而 $p \nmid u_{r-1} \Longrightarrow p^\alpha \mid p^r \Longrightarrow \alpha \leqslant r$，但 $r \leqslant \alpha \Longrightarrow r = \alpha \Longrightarrow \delta = p^{\alpha-1}(p-1) = \varphi(p^\alpha) \Longrightarrow (g + pt_0) \in {}_{p^\alpha}\varphi(p^\alpha)$。

所以 $g + pt_0$ 是模 p^α 的原根。

定理6·7 设 $\alpha \geqslant 1$，g 是模 p^α 的一个原根，则 g 与 $g + p^\alpha$ 中的奇数是模 $2p^\alpha$ 的一个原根。

证明 (i) 若 x 是奇数，则显然当 x 适合同余式

$$x^\gamma \equiv 1 \pmod{p^\alpha} \qquad \text{(a)}$$

时，亦适合同余式

$$x^{\gamma}\equiv 1\ (\mathrm{mod}\ 2p^{\alpha}).\qquad (b)$$

反之，亦显然有，若 x 适合(b)，则 x 亦适合(a)。

(ii) 若 g 是奇数，且

$g^{\varphi(p^{\alpha})}\equiv 1\ (\mathrm{mod}\ p^{\alpha})$，$g^{r}\not\equiv 1\ (\mathrm{mod}\ p^{\alpha})$ $(0\leqslant r<\varphi(p^{\alpha}))$。

则由 $\varphi(p^{\alpha})=\varphi(2p^{\alpha})=p^{\alpha-1}(p-1)$及(i)，即得

$g^{\varphi(2p^{\alpha})}\equiv 1\ (\mathrm{mod}\ 2p^{\alpha})$，$g^{r}\not\equiv 1\ (\mathrm{mod}\ 2p^{\alpha})$ $(0<r<\varphi(2p^{\alpha}))$，故 g 是模 $2p^{\alpha}$ 的一个原根。

(iii) 同理可证，若 $g+p^{\alpha}$ 是奇数，则 $g+p^{\alpha}$ 是模 $2p^{\alpha}$ 的一个原根。

定理6·8 模 m 原根存在的充要条件是：m 等于 2，4，p^{α} 或 $2p^{2\alpha}$，其中 p 是奇素数。

为了证明本定理，先证

引理 当 $n\geqslant 3$，$(a,\ 2^{n})=1$ 时，同余式

$$a^{2^{n-2}}\equiv 1\ (\mathrm{mod}\ 2^{n})\qquad (a)$$

永远成立。

证明 今用数学归纳法证明之。

A) 当 $n=3$ 时，$a=2a_1+1$，所以

$a^2=4a_1(a_1+1)+1\equiv 1\ (\mathrm{mod}\ 2^3)$。

B) 设 $a^{2^{(n-1)-2}}\equiv 1\ (\mathrm{mod}\ 2^{n-1})$，则

$$\begin{aligned} a^{2^{n-2}} &= (a^{2^{n-1-2}})^2=(1+2^{n-1}t)^2 \\ &= 1+2^{n}(t+2^{n-2}t^2) \\ &\equiv 1\ (\mathrm{mod}\ 2^{n}) \end{aligned}$$

所以(a)对于任一 $n\geqslant 3$ 的整数 n 都成立。

因为 $\varphi(2^{n})=2^{n-1}$，所以这个引理说明了模 2^{n} $(n\geqslant 3)$ 无

原根。

定理的证明 (i) 必要条件：设

$$m=2^{n}p_1^{\alpha_1}\cdots p_k^{\alpha_k},$$

是 m 的标准分解式，若 $(a, m)=1$，则 $(a, 2^n)=1$，$(a, p_i^{\alpha_i})=1\ (i=1, \cdots, k)$，由欧拉定理及引理得

$$a^{\varphi(p_i^{\alpha_i})}\equiv 1\ (\mathrm{mod}\,p_i^{\alpha_i})(i=1, \cdots, k); \qquad (b)$$

$$\begin{cases} a^{\varphi(2^n)}\equiv 1\ (\mathrm{mod}\ 2^n), \text{ 当 } n\leqslant 2 \text{ 时;} \\ a^{\frac{1}{2}\varphi(2^n)}\equiv 1\ (\mathrm{mod}\,2^n), \text{ 当 } n\geqslant 3 \text{ 时.} \end{cases} \qquad (c)$$

令

$$\tau=\begin{cases} \varphi(2^n)=2^{n-1}, \text{ 当 } n\leqslant 2 \text{ 时;} \\ \frac{1}{2}\varphi(2^n)=2^{n-2}, \text{ 当 } n\geqslant 3 \text{ 时.} \end{cases}$$

$$h=\left[\tau, \varphi\left(p_1^{\alpha_1}\right), \cdots, \varphi\left(p_k^{\alpha_k}\right)\right].$$

则由(b)，(c)及同余的性质11°，得

$$a^h\equiv 1\ (\mathrm{mod}\ m),$$

既然上式对一切与 m 互素的整数 a 都成立，因此若 $h<\varphi(m)$，则模 m 的原根不存在。所以我们只要讨论何时 $h=\varphi(m)$（这是模 m 有原根的必要条件）。

当 $n\geqslant 3$ 时，

$$h\leqslant\tau\prod_{i=1}^{k}\varphi(p_i^{\alpha_i})=\frac{1}{2}\varphi(m)<\varphi(m),$$

所以 $2^n\mid m(n\geqslant 3)$ 时，模 m 无原根。

当$k>1$时，$2 \mid \varphi(p_1^{\alpha_1})$，$2 \mid \varphi(p_2^{\alpha_2})$，因此

$$[\varphi(p_1^{\alpha_1}), \varphi(p_2^{\alpha_2})] < \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}),$$

$$\therefore \qquad h < \varphi(2^n)\prod_{i=1}^{h}\varphi(p_i^{\alpha_i}) = \varphi(m).$$

所以 m 含有两个或两个以上奇素因子时，没有原根。

当 $n=2$，$k=1$ 时，$\varphi(2^2)=2$，$2 \mid \varphi(p_1^{\alpha_1})$，

$$\therefore \qquad h < \varphi(m).$$

所以 $m=2^2p^\alpha$ 时，没有原根。

归纳上述讨论知，m 有原根的必要条件是，其标准分解式符合下列四种情况之一：

$$\begin{cases} n=1, \\ k=0; \end{cases} \quad \begin{cases} n=2, \\ k=0; \end{cases} \quad \begin{cases} n=0, \\ k=1; \end{cases} \quad \begin{cases} n=1, \\ k=1. \end{cases}$$

(ii) 充分条件：当 $m=2$ 时，$\varphi(2)=1$，1 是模2的原根；当$m=4$时，$\varphi(4)=2$，3 是模4的原根。由定理6·5、6·6、6·7知 $m=p^\alpha$，$2p^\alpha$ $(\alpha \geqslant 1)$时，都有原根。

定理6·9 设 $m>1$，$\varphi(m)$的不同素因子是q_1，q_2，…，q_k，$(g, m)=1$，则 g 是模 m 的一个元根的充要条件是：

$$g^{\frac{\varphi(m)}{q_i}} \not\equiv 1 \pmod{m}, \quad i=1, 2, \cdots, k \qquad (2)$$

证明 (i) 若 $g \in_m \varphi(m)$，但

$$0 < \frac{\varphi(m)}{q_i} < \varphi(m), \quad i=1, 2, \cdots, k$$

所以(2)式成立。

(ii) 若(2)式成立，设 $g \in_m \delta$，今用反证法证明之。

设 $\delta<\varphi(m)$，由定理6·2的系1知 $\delta|\varphi(m)$，且 $\frac{\varphi(m)}{\delta}$ 是大于1的整数，则必有一

$$q_i\left|\frac{\varphi(m)}{\delta}\Longrightarrow\frac{\varphi(m)}{\delta}=q_iu\Longrightarrow\frac{\varphi(m)}{q_i}=\delta u\Longrightarrow\right.$$

$$\Longrightarrow g^{\frac{\varphi(m)}{q_i}}=(g^{\delta})^u\equiv 1\ (\text{mod } m)$$

这与假设矛盾。

定理6·9给予我们求模 $m=p^{\alpha}$ 原根的一种方法：先求出 $\varphi(p^{\alpha})=q_1^{\alpha_1}\cdots q_k^{\alpha_k}$，然后找出一个整数 g，$(g, m)=1$，使它满足(2)式的条件，则这个 g 即所求的原根。

例6·1 设 $m=41$，$\varphi(m)=\varphi(41)=2^3\times 5$，则 $q_1=2$，$q_2=5$，$\frac{\varphi(m)}{2}=20$，$\frac{\varphi(m)}{5}=8$，故 g 是模41的原根的充要条件是：

$$g^{20}\not\equiv 1\ (\text{mod } 41),\quad g^8\not\equiv 1\ (\text{mod } 41),\quad (g, 41)=1.$$

我们用1，2，3，…，40逐一验算，得到

$1^8\equiv 1(\text{mod } 41)$；$\left.\begin{array}{l}2^8\equiv 10(\text{mod } 41),\\ 2^{20}\equiv 1(\text{mod } 41);\end{array}\right\}$ $3^8\equiv 1(\text{mod } 41)$；

$\left.\begin{array}{l}4^8\equiv 18(\text{mod}41),\\ 4^{20}\equiv 1\ (\text{mod}41);\end{array}\right\}$ $\left.\begin{array}{l}5^8\equiv 18(\text{mod}41),\\ 5^{20}\equiv 1\ (\text{mod}41);\end{array}\right\}$

$\left.\begin{array}{l}6^8\equiv 10\not\equiv 1\ (\text{mod}41),\\ 6^{20}\equiv -1\not\equiv 1\ (\text{mod}41).\end{array}\right\}$

故6是模41的一个原根。

例6·2 设 $m=41^2=1681$，此时虽亦可用定理6·9的方法，求模 41^2 的原根。但用定理6·6的方法似更简单。

由例6·1知 $6\in_{41}40$，计算之可得

$6^{40}\equiv 124\ (\text{mod}41^2)\Longrightarrow 6^{40}=1+41(3+41l)$，其

中 l 是正整数。

$(6+41t)^{40}=1+41(3+41l-6^{39}t+41T)=1+41u$，其中 $u=3+41l-6^{39}t+41T$，$T=6^{39}t+C_{41}^{2}6^{38}\cdot 41t^{2}+\cdots+41^{39}t^{40}$。当 $t=0$ 时，$41\nmid u$。故由定理6·6知，$6+41\times 0=6$ 是模41^2的一个原根。

例6·3 设 $m=2\times 41^2=3362$，此时模 m 的原根虽亦可由定理6·9的方法来求得。但由例6·2及定理6·7立即得到 $6+41^2=1687$是模3362的一个原根。

必须引起注意的是，由定理6·9所提供求原根的方法，并不是对任何模 m 都能计算，因为φ(m)的标准分解式不一定都能求出。另一方面，m 很大时，即使能求出 φ(m)的一切素因子，但(2)式的验算亦十分繁杂，这是一个大缺点。

第二节 指数及 n 次剩余

当 $m=p^\alpha$ 或 $m=2p^\alpha$ 的情况下，模 m 的原根是存在的，本节在这个基础上引进指数的概念，并推出它的性质，用以研究同余式

$$x^n\equiv a(\mathrm{mod}\ m),\ (a,\ m)=1$$

有解的条件，有解时解的数量以及如何求解。最后介绍如何求出模 m 的原根的个数。

本节无特别声明时，模 m 都指的是 p^α 或 $2p^\alpha$，$c=\varphi(m)$，g 是模 m 的一个原根。

定理6·10 若 r 通过模 c 的最小非负完全剩余系，则g^r通过模 m 的一个互素剩余系。

证明 因为 g 是模 m 的一个原根，由原根的定义及定理6·1，知

$$g^0,\ g^1,\ g^2,\ \cdots,\ g^{c-1} \qquad (a)$$

是对模 m 两两互不同余的 c 个数。又因 $(g, m) = 1 \Longrightarrow (g^r, m) = 1$，$r = 0, 1, \cdots, c-1$，所以 (a) 是模 m 的互素剩余系。

有了定理6·10，我们可以对于每一个与模 m 互素的数引进“指数”的概念。指数的概念与对数概念很相象，而原根相当于对数的底。

定义6·2 给定的一个整数 a，若对模m的一个原根 g，存在一非负整数 r，使得

$$a \equiv g^r \pmod m$$

成立，则 r 叫做以 g 为底的 a 对模m的一个指数(index)。记作：

$$r = \mathrm{ind}_g a, \text{ 或 } r = \mathrm{ind}\ a.$$

由定义6·2知，a 的指数不仅对模m有关，而且与为底的原根亦有关系。例如，2，3 都是模 5 的原根，但 $\mathrm{ind}_3 3 = 1$，$\mathrm{ind}_2 3 = 3$。

由定理6·10知道，任一与模m互素的整数 a，对于模 m 的任一原根 g 来说，a 的指数都存在；若 $(a, m) \neq 1$，则对模m的任一原根来说，a 的指数都不存在。

以 g 为底 a 对模m的指数，实际上是关于模 c 的一个类中的一切非负整数。

定理6·11 若 $(a, m) = 1$，$g \in {}_m c$，则对模m来说，a 有一个以 g 为底的指数 r'，$0 \leqslant r' < c$，并且以 g 为底 a 对模 m的一切指数是满足

$$r \equiv r' \pmod c, \quad r \geqslant 0$$

的整数 r。

证明 因为 $(a, m) = 1$，所以由定理6·10知道，$\exists r'$，$0 \leqslant r' < c \ni a \equiv g^{r'} \pmod m$。

若 $g^r \equiv a \pmod m\ (r \geqslant 0) \Longrightarrow g^r \equiv g^{r'} \pmod m$。由于 $g \in _m c$，由定理6·2知，

$$r \equiv r' \pmod c,\quad r \geqslant 0\ .$$

反之，若 $r \equiv r' \pmod c$，$r \geqslant 0$，则由定理6·2知

$$g^r \equiv g^{r'} \equiv a \pmod m$$

即满足定理条件的非负整数 r，都是 a 的指数。

定理6·12 若 g 是模m的一个原根，r 是一个非负整数，则以 g 为底，对模m有同一指数 r 的一切整数是模 m的一个与模互素的剩余类。

证明 由定义6·2知道，

$$\mathrm{ind}_g a = r \Longleftrightarrow a \equiv g^r \pmod m,$$

且$(g^r, m) = 1$，所以与m互素的剩余类$\{g^r\}$中的任一数的指数都是 r。

综合上述内容，可得

$$\mathrm{ind}\ a \equiv \mathrm{ind}\ b \pmod c \Longleftrightarrow a \equiv b \pmod m。\qquad (3)$$

下面我们证明一个与对数完全相象的性质：

定理6·13 若 $a_1, a_2, \cdots, a_n$ 是与m互素的 n 个整数，则

$$\mathrm{ind}\ a_1a_2\cdots a_n \equiv \mathrm{ind}\ a_1 + \mathrm{ind}\ a_2 + \cdots + \mathrm{ind}\ a_n \pmod c,$$

特别地，

$$\mathrm{ind}\ a^n \equiv n\ \mathrm{ind}\ a \pmod c。$$

证明 由定义6·2知

$$a_i \equiv g^{\mathrm{ind} a_i} \pmod m,\ i = 1, 2, \cdots, n \Longrightarrow a_1 a_2 \cdots a_n \equiv g^{\mathrm{ind}\ a_1 + \mathrm{ind}\ a_2 + \cdots + \mathrm{ind}\ a_n}.$$

$$\therefore\quad \mathrm{ind}(a_1a_2\cdots a_n) \equiv \mathrm{ind}\ a_1 + \mathrm{ind}\ a_2 + \cdots + \mathrm{ind}\ a_n \pmod c。$$

令　$a_1 = a_2 = \cdots = a_n$，得

$$\text{ind}\,a^n \equiv n\,\text{ind}\,a \pmod{c}.$$

利用指数可以解同余式（1），正象利用对数可以求 n 次方根一样，我们预先要对于模m选出以某一原根为底的两个指数表：一个是已知一数 a，求 a 的指数 r 的表 I；另一个是由指数 r 求其所对应的数 a 的表N。表中所出现的 a 只是模m的最小非负互素的剩余，而 r 是模$\varphi(m)$的最小非负剩余。

例6·4　作模41的两个指数表，由例6·1知 6 是模41的一个原根，因此以 6 为底，计算：

$6^0 \equiv 1$，　$6^1 \equiv 6$，　$6^2 \equiv 36$，　$6^3 \equiv 11$，　$6^4 \equiv 25$，

$6^5 \equiv 27$，　$6^6 \equiv 39$，　$6^7 \equiv 29$，　$6^8 \equiv 10$，　$6^9 \equiv 19$，

$6^{10} \equiv 32$，　$6^{11} \equiv 28$，　$6^{12} \equiv 4$，　$6^{13} \equiv 24$，　$6^{14} \equiv 21$，

$6^{15} \equiv 3$，　$6^{16} \equiv 18$，　$6^{17} \equiv 26$，　$6^{18} \equiv 33$，　$6^{19} \equiv 34$，

$6^{20} \equiv 40$，　$6^{21} \equiv 35$，　$6^{22} \equiv 5$，　$6^{23} \equiv 30$，　$6^{24} \equiv 16$，

$6^{25} \equiv 14$，　$6^{26} \equiv 2$，　$6^{27} \equiv 12$，　$6^{28} \equiv 31$，　$6^{29} \equiv 22$，

$6^{30} \equiv 9$，　$6^{31} \equiv 13$，　$6^{32} \equiv 37$，　$6^{33} \equiv 17$，　$6^{34} \equiv 20$，

$6^{35} \equiv 38$，　$6^{36} \equiv 23$，　$6^{37} \equiv 15$，　$6^{38} \equiv 8$，　$6^{39} \equiv 7$．

因此可列表如下：其中第一纵行是十位数字．

由 a 查 r 的表I

	0	1	2	3	4	5	6	7	8	9
0		0	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9
2	34	14	29	36	13	4	17	5	11	7
3	23	28	10	18	19	21	2	32	35	6
4	20									

由 r 查 a 的表N

	0	1	2	3	4	5	6	7	8	9
0	1	6	36	11	25	27	39	29	10	19
1	32	28	4	24	21	3	18	26	33	34
2	40	35	5	30	16	14	2	12	31	22
3	9	13	37	17	20	38	23	15	8	7

例如，从上面的I表查得30的指数是23，19的指数是9，即$\text{ind}30\equiv23,\text{ind}19\equiv9(\text{mod }40)$；从N表中查得对应于指数21的数是35，对应于指数34的数是20，即 $g^{21}\equiv35$，$g^{20}\equiv34(\text{mod }41)$，其中 $g=6$，等等。

现在应用指数来研究同余式(1)有解的条件．为此先引进

定义6·3 设m是给定的正整数，若同余式(1)有解，则 a 叫做模m的一个 n 次剩余（residue of degree n)；若(1)无解，则 a 叫做模m的一个 n 次非剩余（non-residue of degree n)。

定理6·14 若$(n,c)=d$，$(a,m)=1$，则

(i) 同余式

$$x^n\equiv a(\text{mod }m) \qquad (1)$$

有解（即 a 是对模m的n 次剩余）的充要条件是$d\mid \text{ind }a$，并且有解时其解数是 d。

(ii) 在模m的一个互素剩余系中，n 次剩余的个数是：$\frac{c}{d}$。

证明 由等价关系式(3)与定理6·13，立即得到同余式

$$n\,\mathrm{ind}\,x \equiv \mathrm{ind}\,a \pmod{c} \qquad (4)$$

与同余式（1）等价。即（4）的任一解 $x\equiv x_0 \pmod{m}$，都是（1）的解；反之，（1）的任一解 $x\equiv x_0 \pmod{m}$ 亦（4）的解。今分下面两点来证明：

(i) 由定理6·10知道，对于任一整数X，同余式

$$X\equiv \mathrm{ind}\,x \pmod{c}$$

都有解 x，故（4）有解的充要条件是

$$nX\equiv \mathrm{ind}\,a \pmod{c} \qquad (4')$$

有解。由定理4·1知（4′）有解的充要条件是：

$$d \mid \mathrm{ind}\,a,\quad (n,\ c)=d.$$

并且有解时有 d 个解，所以（1）有解的充要条件是：$d\mid \mathrm{ind}\,a$，且有解时有 d 个解。

(ii) 由(i)知，对模m的 n 次剩余的个数是指数inda的序列

$$0,\ 1,\ 2,\ \cdots,\ c-1$$

中 d 的倍数的个数，故 n 次剩余的个数是$\frac{c}{d}$。

今把二次剩余的欧拉判别条件推广于下：

系 a 对模m的 n 次剩余的充要条件是：

$$a^{\frac{c}{d}}\equiv 1 \pmod{m},\quad d=(n,\ c).$$

证明 由定理6·14知道：

（1）式有解（a为模m的n次剩余）$\Longleftrightarrow \mathrm{ind}\,a\equiv 0 \pmod{d} \overset{d\mid c}{\Longleftrightarrow} \frac{c}{d}\mathrm{ind}\,a\equiv 0 \pmod{c} \overset{(3)}{\Longleftrightarrow} a^{\frac{c}{d}}\equiv 1 \pmod{m}$.

例6·5 在同余式

$$x^8 \equiv 23 \pmod{41} \qquad (a)$$

中，$n=8$，$c=\varphi(41)=40$，$(40, 8)=8$，$\operatorname{ind} 23=36$，因$8 \nmid 36$，故(a)无解。

例6·6 在同余式

$$x^{12} \equiv 37 \pmod{41} \qquad (b)$$

中，$d=(12, 40)=4$，$\operatorname{ind} 37=32$，因$4 \mid 32$，故(b)有解，且其解数为4。又由等价关系式(3)知道，同余式(b)等价于同余式

$$12 \operatorname{ind} x \equiv \operatorname{ind} 37 \pmod{40}.$$

先解

$$3 \operatorname{ind} x \equiv 8 \pmod{10}, \qquad (c)$$

得 $\operatorname{ind} x \equiv 6 \pmod{10}$，故(c)的解是

$$\operatorname{ind} x \equiv 6, 16, 26, 36 \pmod{40}.$$

查N表得 $x \equiv 39, 18, 2, 23 \pmod{41}$ 是(b)的解。

例6·7 $x^4 \equiv a \pmod{41} \overset{(3)}{\Longleftrightarrow} 4 \operatorname{ind} x \equiv \operatorname{ind} a \pmod{40}$。而$(n, c)=(4, 40)=4$，由表I查得，当 a 等于

1，4，10，16，18，23，25，31，37，40

时 $4 \mid \operatorname{ind} a$，所以这10数都是模41的四次剩余。表内看到此外再无别的数了。而$\frac{c}{d}=10$，故它适合定理6·14(ii)的结论。

由于$(4, 40)=(12, 40)=(28, 40)=(36, 40)=4$。故这10个数亦是模41的12次、28次、36次剩余。

定理6·15 若$(a, m)=1$，$a \in_m \delta$，则 $\delta=\dfrac{c}{(\operatorname{ind} a, c)}$。特别是 a 是模m的一个原根的充要条件是：$(\operatorname{ind} a, c)=1$。

证明 因为$a \in_m \delta$，所以$a^\delta \equiv 1 \pmod{m}$，由定理6·13知

$$\delta \operatorname{ind} a \equiv 0 \pmod{c},$$

由定理6·2系1知，$\delta | c$，

$$\therefore \qquad \operatorname{ind} a \equiv 0 \left(\bmod \frac{c}{\delta}\right),$$

即$\frac{c}{\delta} | \operatorname{ind} a$，而$\frac{c}{\delta} | c$，故$\frac{c}{\delta} | (\operatorname{ind} a, c)$，因此

$$\frac{c}{\delta} \leqslant (\operatorname{ind} a, c) \Longrightarrow \frac{c}{(\operatorname{ind} a, c)} \leqslant \delta. \qquad (\alpha)$$

命 $d = (\operatorname{ind} a, c)$，则

$$\operatorname{ind} a \equiv 0 \pmod{d} \Longrightarrow \frac{c}{d} \operatorname{ind} a \equiv 0 \pmod{c} \Longrightarrow a^{\frac{c}{d}}$$

$$\equiv 1 \pmod{m} \overset{\delta\text{的定义}}{\Longrightarrow} \delta \leqslant \frac{c}{d} = \frac{c}{(\operatorname{ind} a, c)},$$

结合(α)，得

$$\delta = \frac{c}{(\operatorname{ind} a, c)}.$$

若 $a \in_m c$，则 $\delta = c \Longrightarrow (\operatorname{ind} a, c) = 1$.

反之，若$(\operatorname{ind} a, c) = 1$，则 $a \in_m c$，即 a 是模 m的原根.

注意：从证明的过程可以看出：不论以模m的那一个原根为底，定理6·15的结论都是一样的.

定理6·16 在模m的互素剩余系中，属于方次数δ的整数的个数是$\varphi(\delta)$，特别地，在模m的互素剩余系中，原根的个数是$\varphi(c)$.

证明 设在模m的互素剩余系中，属于方次数δ的整数的个数是T，则由定理6·15知T等于在模m的互素剩余系中，满足条件

$$(\operatorname{ind} a, c) = \frac{c}{\delta}$$

的 a 的个数。由于当 x 过模m的互素剩余系时，ind x过模c的完全剩余系，故T等于满足条件

$$(y,\ c)=\frac{c}{\delta},\quad 0\leqslant y<c$$

的整数 y 的个数，令 $y=\frac{c}{\delta}u$，因为$(\frac{c}{\delta}u,\ c)=\frac{c}{\delta}(u,\ \delta)=\frac{c}{\delta}$，所以T等于满足条件$(u,\ \delta)=1$，$0\leqslant u<\delta$的整数u的个数。

$\therefore\qquad T=\varphi(\delta)$。

特别地，在模m的互素剩余系中，属于方次数c的整数的个数是$\varphi(c)$，故模m原根的个数是$\varphi(c)$。

此定理解决了原根的数量的问题。

例6·8 在模41的互素剩余系中，属于方次数10的数a满足条件

$$(\text{ind}\ a,\ 40)=\frac{40}{10}=4\Longrightarrow \text{ind}\ a=4,\ 12,\ 28,\ 36\Longrightarrow a=25,\ 4,\ 31,\ 23.\ a\in_{41}10,$$

其个数是$\varphi(10)=4$。

例6·9 在模41的互素剩余系中，原根是适合条件

$$(\text{ind}\ a,\ 40)=1$$

的数a，即

$$\text{ind}\ a=1,\ 3,\ 7,\ 9,\ 11,\ 13,\ 17,\ 19,\ 21,\ 23,\ 27,\ 29,\ 31,\ 33,\ 37,\ 39$$

$$\Longrightarrow a=6,\ 11,\ 29,\ 19,\ 28,\ 24,\ 26,\ 34,\ 35,\ 30,\ 12,\ 22,\ 13,\ 17,\ 15,\ 7.$$

这$16=\varphi(40)$个数都是模41的原根。

书末附有4000以下的素数及其最小原根表，以及100以

内素数模的原根及指数表（由 a 查 r 用"I"表，由 r 查 a 用"N"表）。

与对数换底公式类似地，有

定理6·17 若 g_1 和 g_2 是模m的两个原根，（a，m）= 1，则

$$\left.\begin{aligned}\text{ind}_{g_1} a &\equiv \text{ind}_{g_2} a \times \text{ind}_{g_1} g_2 \pmod c\\ \text{ind}_{g_2} a &\equiv \text{ind}_{g_1} a \times \text{ind}_{g_2} g_1 \pmod c\end{aligned}\right\} \tag{6}$$

并且

$$\text{ind}_{g_2} g_1 \times \text{ind}_{g_1} g_2 \equiv 1 \pmod c, \quad c = \varphi(m) \tag{7}$$

证明 设 $\alpha_1 \equiv \text{ind}_{g_1} a$，$\alpha_2 \equiv \text{ind}_{g_2} a \pmod c$，

$\therefore$ $a \equiv g_1^{\alpha_1} \equiv g_2^{\alpha_2} \pmod m \Longrightarrow \text{ind}_{g_1} g_1^{\alpha_1}$

$\equiv \text{ind}_{g_1} g_2^{\alpha_2} \pmod c \Longrightarrow \alpha_1 \equiv \alpha_2 \text{ind}_{g_1} g_2 \pmod c \Longrightarrow$

$\text{ind}_{g_1} a \equiv \text{ind}_{g_2} a \times \text{ind}_{g_1} g_2 \pmod c$。

同理，

$\text{ind}_{g_2} g_1^{\alpha_1} \equiv \text{ind}_{g_2} g_2^{\alpha_2} \Longrightarrow \text{ind}_{g_2} a \equiv \text{ind}_{g_1} a$

$\times \text{ind}_{g_2} g_1 \pmod c$。

在（6）的第一式中取 $a = g_1$，就得到（7）。

表达式 $\text{ind}_{g_1} g_2$ 或 $\text{ind}_{g_2} g_1$ 与对数理论中所谓"模"相仿。

例6·10 计算 $\text{ind}_{15} 13 \equiv ?\ (\text{mod}\ \varphi(19))$。

解 在模 19 的 I 表中查得，$\text{ind}_{10} 13 \equiv 13 \pmod{18}$，$\text{ind}_{10} 15 \equiv 7 \pmod{18}$，由公式（6）得

$ind_{10}13 \equiv ind_{15}13 \cdot ind_{10}15 \pmod{18}$

$\Longrightarrow 7ind_{15}13 \equiv 13 \pmod{18}$.

解得 $ind_{15}13 \equiv 7 \pmod{18}$.

例6·11 解下诸同余式：

(i) $36x \equiv 57 \pmod{83}$； (ii) $8x \equiv -21 \pmod{47}$；

(iii) $x^2 \equiv 31 \pmod{43}$； (iv) $x^2 \equiv 23 \pmod{97}$；

(v) $x^3 \equiv 7 \pmod{29}$； (vi) $x^5 \equiv -3 \pmod{41}$；

(vii) $x^6 \equiv 69 \pmod{71}$； (viii) $x^6 \equiv 3 \pmod{71}$.

解 正如应用对数知识解方程一样地，把方程的两边"取对数"，改为在已知同余式两边"取指数"，把一般同余式改变成指数的同余式.

(i) 两边取指数得

$ind\ 36 + ind\ x \equiv ind\ 57 \pmod{82}$

从素数83的I表中查得：$ind\ 36 = 28$，$ind\ 57 = 29$.

$\therefore\ ind\ x \equiv 1 \pmod{82}$

查N表得，$x \equiv 50 \pmod{83}$.

(ii) $8x \equiv 26 \pmod{47} \Longrightarrow 4x \equiv 13 \pmod{47}$

$\overset{\text{取指数}}{\Longrightarrow} ind\ 4 + ind\ x \equiv ind\ 13 \pmod{46}$

$\overset{\text{查I表}}{\Longrightarrow} 14 + ind x \equiv 3 \pmod{46} \Longrightarrow ind\ x \equiv 35 \pmod{46}$

$\overset{\text{查N表}}{\Longrightarrow} x \equiv 15 \pmod{47}$.

(iii) $x^2 \equiv 31 \pmod{43} \overset{\text{取指数}}{\Longrightarrow} 2ind\ x \equiv ind\ 31 \pmod{42}$

$\overset{\text{查I表}}{\Longrightarrow} 2ind\ x \equiv 32 \pmod{42} \Longrightarrow ind\ x \equiv 16 \pmod{21}$

$\Longrightarrow ind\ x_1 \equiv 16 \pmod{42}$，$ind\ x_2 \equiv 37 \pmod{42}$

$\overset{\text{查N表}}{\Longrightarrow} x_1 \equiv 17$，$x_2 \equiv 26 \pmod{43}$

(iv) $x^2\equiv 23 \pmod{97} \Longrightarrow 2\text{ind}\,x\equiv \text{ind}\,23\equiv 79 \pmod{96}$ 而（2，96）＝2，$2\nmid 79$，故原同余式无解．即 $\left(\frac{23}{79}\right)=-1$．

(v) $x^3\equiv 7 \pmod{29} \Longrightarrow 3\text{ind}\,x\equiv \text{ind}\,7\equiv 20 \pmod{28} \Longrightarrow \text{ind}\,x\equiv 16 \pmod{28} \Longrightarrow x\equiv 16 \pmod{29}$．
因（3，28）＝1，故它是原同余式的唯一解．

(vi) 因（5，40）＝5，故原同余式有解时，有五个解．用38代－3后，同余式两边取指数得

$$5\,\text{ind}\,x\equiv \text{ind}\,38\equiv 35 \pmod{40}$$

$$\text{ind}\,x\equiv 7 \pmod{8},$$

$\therefore$ $\text{ind}\,x\equiv 7，15，23，31，39 \pmod{40}$
查N表得

$x\equiv 29，3，30，13，7 \pmod{41}$

是原同余式的五个解．

(vii) 因(6，70)＝2，故有解时有二解，但

$$6\,\text{ind}\,x\equiv \text{ind}\,69\equiv 23 \pmod{70}$$

无解，故原同余式无解．

(viii) 因(6，70)＝2，故有解时有二解，而

$6\text{ind}\,x\equiv \text{ind}\,3\equiv 18 \pmod{70} \Longrightarrow 3\text{ind}\,x\equiv 9 \pmod{35} \Longrightarrow \text{ind}\,x\equiv 3 \pmod{35} \Longrightarrow \text{ind}\,x\equiv 3，38 \pmod{70} \Longrightarrow x\equiv 52，19 \pmod{71}$

是原同余式的两个解．

第三节　指数组及解合数模同余式

上节研究了指数的基本性质及其对解素数模n次二项同余式的应用．但是指数的概念有赖于模m的原根的存在，在

第一节中知道当且仅当 $m=2, 4, p^\alpha, 2p^\alpha$（p是奇素数，$\alpha$ 是自然数）时，模m的原根存在。m在一般的情况下，原根往往不存在，此时 $x^n \equiv a \pmod m$ 是否有解？有解时如何求解？为此本节将对一般情况的模 m 引入"指数组"的概念，进而探讨 $x^n \equiv a \pmod m$ 的求解问题。

从定理6·8的引理知道，当 $\alpha \geqslant 3$，$(a, 2^\alpha)=1$ 时，都有

$$a^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}。\qquad (8)$$

下面将研究是否存在整数 a，它对模 $2^\alpha(\alpha \geqslant 3)$ 是属于方次数 $2^{\alpha-2}$？其答案是肯定的。

定理6·18 设 $\alpha \geqslant 3$，则 $5 \in_{2^\alpha} 2^{\alpha-2}$，并且

$$\pm 5^0, \ \pm 5^1, \ \pm 5^2, \ \cdots, \ \pm 5^{2^{\alpha-2}-1} \qquad (9)$$

是模 2^α 的一个互素剩余系。

证明 设 5 对模 2^α 是属于方次数 δ，由(8)及定理6·2即得 $\delta \mid 2^{\alpha-2}$，亦即 $\delta=2^n(0 \leqslant n \leqslant \alpha-2)$，故要证 $\delta=2^{\alpha-2}$，只要证

$$5^{2^m} \not\equiv 1 \pmod{2^\alpha}, \quad 0 \leqslant m < \alpha-2 \qquad (a)$$

就可以了。为此我们先证，对于任意非负整数 m，下列等式成立：

$$5^{2^m} = 1 + 2^{m+2} + 2^{m+3}u_m, \qquad (b)$$

其中 u_m 是一个非负整数。事实上，当 $m=0, 1$ 时，$u_0=0$，$u_1=1$。当 $m>1$ 时，

$$5^{2^m} = (1+2^2)^{2^m} = 1 + 2^{m+2} + \frac{2^m(2^m-1)}{2} \cdot 2^4 + \cdots$$

$$+ (2^2)^{2^m} = 1 + 2^{m+2} + 2^{m+3}u_m, \qquad (b')$$

其中 $u_m = \left[(2^m - 1) + \frac{(2^m-1)(2^m-2)}{3} \cdot 2^2 + \cdots + 2^{2^{m+1}-(m+3)} \right] (m \geqslant 2)$，是一个正整数。

由(b′)得

$$5^{2^m} \equiv 1 (\bmod\ 2^{m+2}) \text{且} 5^{2^m} \not\equiv 1 (\bmod 2^\alpha).$$

其中 $0 \leqslant m < \alpha - 2$，即 $2 \leqslant m + 2 < \alpha$。

$\therefore \quad 5 \in {}_2\alpha 2^{\alpha-2}$

再由定理6·1知，下列$2^{\alpha-2}$个数，

$$-5^0,\ 5^1,\ 5^2,\ \cdots,\ 5^{2^{\alpha-2}-1}, \tag{c}$$

对模2^α是两两互不同余的，因而

$$5^0,\ -5^1,\ -5^2,\ \cdots,\ -5^{2^{\alpha-2}-1}, \tag{d}$$

对模2^α亦两两互不同余。不仅如此，(c)中的任一数对(d)中任一数，关于模2^α亦两两互不同余。事实上，因为 $5^s \equiv 1 (\bmod\ 4)$，而 $-5^{s'} \equiv -1 (\bmod 4)$，所以 $5^s \not\equiv -5^{s'} (\bmod 4)$，即$5^s \not\equiv -5^{s'} (\bmod\ 2^\alpha)$，$\alpha \geqslant 2$。

又(c)，(d)中任一数都与 2^α 互素，且其数目是 $2 \cdot 2^{\alpha-2} = 2^{\alpha-1} = \varphi(2^\alpha)$个。所以(9)是模$2^\alpha$的一个互素剩余系。

系　令

$$c = \begin{cases} 1, & \text{当}\alpha = 1\text{时}; \\ 2, & \text{当}\alpha \geqslant 2\text{时}. \end{cases} \qquad c_0 = \begin{cases} 1, & \text{当}\ \alpha = 1\text{时}; \\ 2^{\alpha-2}, & \text{当}\alpha \geqslant 2\text{时}. \end{cases}$$

若 r 及r_0分别过模 c 及 c_0 的最小非负完全剩余系，即

$$r = 0,\ 1,\ \cdots c-1;\quad r_0 = 0,\ 1,\ \cdots,\ c_0 - 1 \tag{a}$$

则$(-1)^r 5^{r_0}$过模2^α的一个互素剩余系。

证明 由定理6·18知道，当$\alpha \geqslant 3$，系的结论成立。当$\alpha=1$时，r和r_0都只能是0，而$(-1)^0 5^0=1$是模2的互素剩余系。当$\alpha=2$时，$r=0, 1$；$r_0=0$。$(-1)^r 5^{r_0}$通过：$(-1)^0 5^0=1$，$(-1)^1 5^0=-1$二数，这是模$2^2=4$的一个互素剩余系。

定理6·19 同余式

$$(-1)^r 5^{r_0} \equiv (-1)^{r'} 5^{r_0'} \pmod{2^\alpha} \tag{10}$$

成立的充分且必要条件是：

$$r \equiv r' \pmod{c}, \quad r_0 \equiv r_0' \pmod{c_0}. \tag{11}$$

证明 设Y，Y′对模c的最小非负剩余分别是s，s′；r_0，r_0'对模c_0的最小非负剩余分别是s_0，s_0'。则由定理6·2知

$$\Longleftrightarrow (-1)^s 5^{s_0} \equiv (-1)^{s_0'} 5^{s_0'} \pmod{2^\alpha}$$

$$(-1)^r 5^{r_0} \equiv (-1)^{r'} 5^{r_0'} \pmod{2^\alpha}$$

由定理6·18系知上式成立的充要条件是

$$r=r', \quad r_0=r_0'$$

即$r \equiv r' \pmod{c}$，$r_0 \equiv r_0' \pmod{c_0}$

现在我们引入模2^α的指数组的概念：

定义6·4 若非负整数r，r_0，使

$$a \equiv (-1)^r 5^{r_0} \pmod{2^\alpha},$$

则 r，r_0 叫做 a 对模2^α 的一个指数组(the system of indices of a to modulus 2^α)。

由定理6·18的系知道，每一与2^α互素的数，对模2^α 有一个指数组 r'，r'_0，且$0 \leqslant r' < c$，$0 \leqslant r'_0 < c_0$。

如果知道 a 对模2^α 的一个指数组是r'，r'_0，那末由定理6·19知，a 对模2^α 的一切指数组是适合条件

$$r \equiv r' \pmod{c},\quad r_0 \equiv r'_0 \pmod{c_0}$$

的一切非负整数对 r，r_0。

由定义6·4还可以直接看出：对模2^α 有同一指数组的一切数，作成一个模2^α的互素剩余类。对于模2^α的指数组，我们还可以得出与定理6·13类似的结果，即

定理6·20 设a_1，a_2，…，a_n是 n 个与2^α 互素的整数 $r(a_i)$，$r_0(a_i)$（$i=1$，2，…，n）是a_i 对模 2^α 的指数组，则 $\sum\limits_{i=1}^{n} r(a_i)$，$\sum\limits_{i=1}^{n} r_0(a_i)$是$a_1a_2\cdots a_n$对模 2^α的一个指数组。

证明 由定义6·4，知

$$a_i \equiv (-1)^{r(a_i)} \cdot 5^{r_0(a_i)} \pmod{2^\alpha}\ (i=1,2,\cdots,n),$$

$$\therefore\ a_1a_2\cdots a_n \equiv (-1)^{\sum\limits_{i=1}^{n} r(a_i)} \cdot 5^{\sum\limits_{i=1}^{n} r_0(a_i)} \pmod{2^\alpha}.$$

再由定理6·4得，$a_1a_2\cdots a_n$ 对模 2^α 的指数组是：

$$\sum_{i=1}^{n} r(a_i),\quad \sum_{i=1}^{n} r_0(a_i).$$

下面我们对一般合数模 $m=2^{\alpha}p_1^{\alpha_1}\cdots p_k^{\alpha_k}$(本节下面的 m 都表示这样的整数)，引入指数组的概念，设 c，c° 的意义与定理6·18的系中的 c，c_0 相同；令 $c_s=\varphi\left(p_s^{\alpha_s}\right)$ $(s=1,\cdots,k)$，g_s是模 $p_s^{\alpha_s}$的最小原根。

定义6·5 若非负整数 r，r_0，r_1，…，r_k，使

$$\left.\begin{aligned} &a\equiv(-1)^{r}\,5^{r_0}\pmod{2^{\alpha}},\\ &a\equiv g_s^{r_s}\left(\bmod\ p_s^{\alpha_s}\right)(s=1,\cdots,k).\end{aligned}\right\}\qquad(12)$$

则 r，r_0，$r_1\cdots$，r_k 叫做 a 对模 m 的一个指数组。

例如，$a=3$，$m=224=2^5\times7$。则

$$3\equiv(-1)^{r}\,5^{r_0}\pmod{2^5}\Longrightarrow r=1,\ r_0=3;$$

$$3\equiv3^{r_1}\pmod 7\Longrightarrow r_1=1.$$

若把它改为 7 的另一个元根 5，则

$$3\equiv5^5\pmod 7\Longrightarrow r_1=5.$$

注意：由于 a 的指数组，与 g_s 的选择有关，为了方便，故在定义6·5中，g_s 取模$p_s^{\alpha_s}$的最小原根，但是若改为任一原根，虽然不同的原根，a 关于模 m 所对应的指数组不同，却不影响下列诸定理的正确性，以及它们在解同余式中的应用。

从定义6·5容易得到下列三条与本节前面定理类似的定理。

定理6·21 若 a 是任一与 m 互素的整数，则 a 有一个对模 m 的指数组 r'，r'_0，r'_1，…，r'_k，$0\leqslant r'<c$，$0\leqslant r'_s<$

$<c_s$，$s=0, 1, \cdots, k$，并且 a 对模m 的一切指数组，都是由适合条件：

$$r\equiv r'(\bmod c), r_s\equiv r_s' (\bmod c_s), \quad s=0,1,\cdots,k \tag{13}$$

的数组 $r, r_0, r_1, \cdots, r_k$ 组成。

证明 因为$(a, m)=1$，所以$(a, 2^\alpha)=1$，$\left(a, p_s^{\alpha_s}\right)=1$，$s=1, 2, \cdots, k$。由定理6·18的系知道，a 有一个对模$2^\alpha$的指数组$r'$，$r_0'$；又由于模 $p_1^{\alpha_1}$，$p_2^{\alpha_2}$，$\cdots$，$p_k^{\alpha_k}$ 的原根都存在，设它们的最小原根分别为 $g_1, g_2, \cdots, g_k$。则由定理6·11知，$\exists r_1', \cdots, r_k'$ 𝗓 $a\equiv g_1^{r_1'} (\bmod p_1^{\alpha_1})$，$\cdots$，

$a\equiv g_k^{r_k'}(\bmod\ p_k^{\alpha_k})$。由定义6·5知，$r'$，$r_0'$，$r_1'$，$\cdots$，$r_k'$是 a 对模 m 的一个指数组。

又由定理6·11及6·19知道，a 对模 m的一切指数组，都是由适合条件(13)的数组 $r, r_0, r_1, \cdots, r_k$ 组成。

定理6·22 任给一个非负整数组 $r, r_0, r_1, \cdots, r_k$，则以这个数组为对模 m 的指数组的一切数，作成一个与模 m 互素的剩余类。

证明 由孙子定理知同余式组

$$x\equiv(-1)^r 5^{r_0} (\bmod 2^\alpha),$$

$$x\equiv g_s^{r_s} (\bmod p_s^{\alpha_s})(s=1, \cdots, k).$$

有唯一解 $x\equiv a(\bmod m)$。又因$(a, 2^\alpha)=\left((-1)^r 5^{r_0}, 2^\alpha\right)=1$，$\left(a, p_s^{\alpha_s}\right)=\left(g_s^{r_s}, p_s^{\alpha_s}\right)=1(s=1, 2, \cdots, k)$，所以

$(a, m)=1$，因而$\{a\}$是对于模 m 互素的一个剩余类。

系 若 $r, r_0, r_1, \cdots, r_k$ 分别过模 $c, c_0, c_1, \cdots, c_k$ 的完全剩余系时，则对应指数组$(r, r_0, \cdots, r_k)$的 a 过模 m 的互素剩余系，其中 $m=2^{\alpha}p_1^{\alpha_1}\cdots p_k^{\alpha_k}$，$c$，$c_0$ 与定理6·18的系里的意义一致，$c_i=\varphi\left(p_i^{\alpha_i}\right)(i=1, \cdots, k)$。

证明 由定理6·18的系及定理6·10知道，

$$r\not\equiv r'(\bmod c)\text{或}r_0\not\equiv r_0'(\bmod c_0)\Longleftrightarrow(-1)^r 5^{r_0}$$

$$\not\equiv(-1)^{r'}5^{r_0'}(\bmod 2^{\alpha});$$

$$r_i\not\equiv r_i'(\bmod c_i)\Longleftrightarrow g_i^{r_i}\not\equiv g_i^{r_i'}(\bmod p_i^{\alpha_i})(i=1,\cdots,k).$$

即任给$(a, m)=1$的 a 时，有且只有一个指数组$(r, r_0, r_1, \cdots, r_k)$使

$$a\equiv(-1)^r 5^{r_0}(\bmod 2^{\alpha}),\quad a\equiv g_i^{r_i}(\bmod p_i^{\alpha_i})$$
$$(i=1, \cdots, k).\qquad(\alpha)$$

反之，对给定的指数组$(r, r_0, r_1, \cdots, r_k)$，由孙子定理知，$(\alpha)$有且只有一个解 a，$(a, m)=1$，这样的指数组与它所对应的 a 都刚好有$\varphi(m)$个，故系里的结论是正确的。

定理6·23 若$(a_i, m)=1(i=1, \cdots, n)$；$r(a_i)$，$r_0(a_i)$，$r_1(a_i), \cdots, r_k(a_i)(i=1, \cdots, n)$是 a_i 对模 m 的指数组，则

$$\sum_{i=1}^{n}r(a_i),\quad \sum_{i=1}^{n}r_0(a_i),\quad \sum_{i=1}^{n}r_1(a_i),\cdots,\sum_{i=1}^{n}r_k(a_i)\qquad(14)$$

是 $a_1a_2\cdots a_n$ 对模 m 的一个指数组。

证明 由定义6·5得

$$\left.\begin{array}{l} a_i \equiv (-1)^{r(a_i)} 5^{r_0(a_i)} \pmod{2^\alpha} \\ a_i \equiv g_s^{r_s(a_i)} \pmod{p_s^{\alpha_s}} (s=1, \cdots, k) \end{array}\right\} i=1, \cdots, n.$$

由定理6·13及6·20知道(14)是 $a_1a_2\cdots a_n$ 对模m一个指数组。

最后我们应用指数组的性质来解同余式。

例6·12 解同余式：$7x\equiv 11 \pmod{16}$。

解 我们先编造模$16=2^4$的指数组表如下：

数 a	1	3	5	7	9	11	13	15
指数 r	0	1	0	1	0	1	0	1
指数r_0	0	3	1	2	2	1	3	0

其中 $r=0,1$；$r_0=0, 1, \cdots, 2^{4-2}-1=0, 1, 2, 3$；

$a\equiv(-1)^r 5^{r_0} \pmod{2^4}$。如，$7\equiv(-1)^1 5^2 \pmod{16}$。

由此先把$7x\equiv 11 \pmod{16}$换成指数组的关系式，由定理6·23知道，7的指数组与x的指数组之“和”应与11的指数组关于模c，c_0同余，所以由上表查得

$1+r\equiv 1 \pmod 2$；$2+r_0\equiv 1 \pmod 4$

因而$r=0$，$r_0=3$，即$x\equiv(-1)^0 5^3\equiv -3 \pmod{16}$是原同余式的解。

例6·13 解同余式

$$x^2\equiv 46 \pmod{105} \tag{a}$$

解 $m=105=3\times5\times7$；$\varphi(m)\equiv\varphi(3)\varphi(5)\varphi(7)=48$。因此105的互素剩余类共有48个，并且3，5，7分别有原根$g_1=2$，$g_2=2$，$g_3=3$。依此造表如下：

数 a，（a，105）=1	1	2	4	8	11	13	16	17	19	22	23	26	29	31
对模 3 的指数r_1	0	1	0	1	1	0	0	1	0	0	1	1	1	0
对模 5 的指数r_2	0	1	2	3	0	3	0	1	2	1	3	0	2	0
对模 7 的指数r_3	0	2	4	0	4	3	2	1	5	0	2	5	0	1

a	32	34	37	38	41	43	44	46	47	52	53	58	59	61	62	64	67	68	71
r_1	1	0	0	1	1	0	1	0	1	0	1	0	1	0	1	0	0	1	1
r_2	1	2	1	3	0	3	2	0	1	1	3	3	2	0	1	2	1	3	0
r_3	4	3	2	1	3	0	2	4	5	1	4	2	1	5	3	0	4	5	0

a	73	74	76	79	82	83	86	88	89	92	94	97	101	103	104
r_1	0	1	0	0	0	1	1	0	1	1	0	0	1	0	1
r_2	3	2	0	2	1	3	0	3	2	1	2	1	0	3	2
r_3	1	4	3	2	5	3	2	4	5	0	1	3	1	5	3

其造表方法可用孙子定理，取48个指数组中的任一个(r_1, r_2, r_3)，求出$a\equiv 2^{r_1} \pmod 3$，$a\equiv 2^{r_2} \pmod 5$，$a\equiv 3^{r_3} \pmod 7$右边的数值；再从

$$a\equiv 70\times 2^{r_1}+21\times 2^{r_2}+15\times 3^{r_3} \pmod{105}$$

中求出非负最小剩余a．例如$a\equiv 2^1\equiv 2 \pmod 3$，$a\equiv 2^3\equiv 3 \pmod 5$，$a\equiv 3^2\equiv 2 \pmod 7$。

$\therefore \quad a \equiv 70\times 2+21\times 3+15\times 2\equiv 23 \pmod{105}$.

所以从而得到23的指数组是(1，3，2)等等.又如，指数组为(1，3，5)的数是：

$$a\equiv 70\times 2+21\times 3+15\times 5\equiv 68 \pmod{105}.$$

由定理6·22的系知道，指数组(r_1, r_2, r_3)与a之间建立了一一对应关系，可造表于上．又如，在表内查得

$$a=4\longrightarrow(r_1, r_2, r_3)=(0, 2, 4);$$

$$a=103\longrightarrow(r_1, r_2, r_3)=(0, 3, 5).$$

即

$$2^0\equiv 4 \pmod 3,\quad 2^2\equiv 4 \pmod 5,\quad 3^4\equiv 4 \pmod 7;$$

$$2^0\equiv 103 \pmod 3,\quad 2^3\equiv 103 \pmod 5,\quad 3^5\equiv 103 \pmod 7.$$

又如，

$$\left.\begin{array}{ll} a_1\equiv 2\equiv 2^1 \pmod 3, & a_1\equiv 1\equiv 2^0 \pmod 5, \\ & a_1\equiv 1\equiv 3^0 \pmod 7; \\ a_2\equiv 1\equiv 2^0 \pmod 3, & a_2\equiv 2\equiv 2^1 \pmod 5, \\ & a_2\equiv 1\equiv 3^0 \pmod 7; \\ a_3\equiv 1\equiv 2^0 \pmod 3, & a_3\equiv 1\equiv 2^0 \pmod 5, \\ & a_3\equiv 3\equiv 3^1 \pmod 7. \end{array}\right\}^* \tag{15}$$

查表得：$a_1\equiv 71$，$a_2\equiv 22$，$a_3\equiv 31 \pmod{105}$．这三个数有下列特点：

$$a_i\equiv g_i\left(\bmod p_i^{\alpha_i}\right),\quad a_i\equiv 1\left(\bmod p_i^{\alpha_i}\right)(j\neq i),$$

$$m=p_1^{\alpha_1}\cdots p_k^{\alpha_k}. \tag{16}$$

其中p_s表示奇素数，本例中$p_1^{\alpha_1}=3$，$p_2^{\alpha_2}=5$，$p_3^{\alpha_3}=7$．

(16)中的a_1，…，a_k叫做与模m互素的诸数的基(base)．亦即，若$(a, m)=1$，$a\to(r_1, \cdots, r_k)$，r_i $(i=1, \cdots, k)$

对模 $\varphi\left(p_i^{\alpha_i}\right)$是唯一确定的，则$a\equiv a_1^{r_1}\cdots a_k^{r_k}\pmod{m}$*．事实上，由于

$$a\equiv a_1^{r_1}\ a_2^{r_2}\cdots a_k^{r_k}\equiv a_i^{r_i}\equiv g_i^{r_i}\pmod{p_i^{\alpha_i}}(i=1,\cdots,k).$$

由定理6·10知道，r_i 是0，1，…，$\varphi\left(p_i^{\alpha_i}\right)-1$中一个唯一确定的数。

由此可见：与105互素的任何数a，都可以从下式中指数组(r_1，r_2，r_3)的取值来确定：

$$a\equiv 71^{r_1}\cdot 22^{r_2}\cdot 31^{r_3}\pmod{105}.$$

其中 $r_1=0$，1；$r_2=0$，1，2，3；$r_3=0$，1，…，5之一．

---

*若$m=2^{\alpha}p_1^{\alpha_1}\cdots p_k^{\alpha_k}$，$\alpha>0$时，则(15)改写为

$$\begin{aligned}
&a_0\equiv-5\equiv(-1)^1 5^1\pmod{2^{\alpha}},a_1\equiv 1\equiv g_1^0\pmod{p_1^{\alpha_1}},\cdots,\\
&\quad a_k\equiv 1\equiv g_k^0\pmod{p_k^{\alpha_k}};\\
&a_0\equiv 1\equiv(-1)^0 5^0)\bmod 2^{\alpha}),a_1\equiv g_1\equiv g_1^1\pmod{p_1^{\alpha_1}},\ \cdots,\\
&\quad a_k\equiv 1\equiv g_k^0\pmod{p_k^{\alpha_k}};\qquad\qquad (15)'\\
&\cdots\cdots\cdots\cdots\cdots\cdots;\\
&a_0\equiv 1\equiv(-1)^0 5^0\pmod{2^{\alpha}},a_1\equiv 1\equiv g_1^0\pmod{p_1^{\alpha_1}},\cdots,\\
&\quad a_k\equiv g_k\equiv g_k^1\pmod{p_k^{\alpha_k}};
\end{aligned}$$

这时模 m 互素诸数的基是 a_0，a_1，…，a_k。a $\Longleftrightarrow$(r，r_0，r_1，…，r_k)都有

$$a\equiv a_0^{(r,r_0)}\ a_1^{r_1}\cdots a_k^{r_k}\pmod{m}\Longrightarrow a\equiv a_0^{(r,r_0)}$$

$$\equiv(-1)^r 5^{r_0}\pmod{2^{\alpha}},a\equiv g_1^{r_1}\pmod{p_1^{\alpha_1}},\ \cdots,$$

$$a\equiv g_k^{r_k}\pmod{p_k^{\alpha_k}}.$$

这又是一种造上表的方法（从 r_i 求 a）。但是此法比用孙子定理的计算量更大，如，$(r_1, r_2, r_3)=(1, 3, 5)$，则

$$a \equiv 71\times 22^3\times 31^5 = 71\times 10648\times 961\times 29791$$
$$\equiv 71\times 43\times 16\times 76 \equiv 8\times 61 \equiv 68 \pmod{105}.$$

今利用所造之表，来解同余式(a)。

由于(a)等价（同解）于同余式组：

$$\begin{cases} x^2 \equiv 46 \equiv 1 \pmod 3, \\ x^2 \equiv 46 \equiv 1 \pmod 5, \\ x^2 \equiv 46 \equiv 4 \pmod 7. \end{cases} \quad \text{(b)}$$

(b)的各同余式两边取指数得

$$\begin{cases} 2\,\mathrm{ind}\,x \equiv 0 \pmod 2, \\ 2\,\mathrm{ind}\,x \equiv 0 \pmod 4, \\ 2\,\mathrm{ind}\,x \equiv \mathrm{ind}\,4 \equiv 4 \pmod 6. \end{cases} \Longrightarrow \begin{cases} 2r_1 \equiv 0 \pmod 2, \\ 2r_2 \equiv 0 \pmod 4, \\ 2r_3 \equiv 4 \pmod 6. \end{cases} \quad \text{(c)}$$

(c)中每一个同余式都有二解：$r_1\equiv 0$，$1 \pmod 2$，$r_2 \equiv 0$，$2 \pmod 4$，$r_3\equiv 2$，$5 \pmod 6$。搭配起来有八个指数组：(0，0，2)，(0，0，5)，(0，2，2)，(0，2，5)，(1，0，2)，(1，0，5)，(1，2，2)，(1，2，5)。每个组合从上表查到的对应值依次是：16，61，79，19，86，26，44，89，就是(a)的八个解。

第四节　特征函数

从前面三节看到了，原根与指数的概念与性质在研究同余式和分数化小数的问题中是很有用的。借助这两个概念，还可以引进在解析数论中很常用的特征函数的概念，本节将初步讨论特征函数的概念及其最基本的性质。

本节采用：$m=2^{\alpha}p_1^{\alpha_1}\cdots p_k^{\alpha_k}(m>1)$是m的标准分解式；c，$c_0$与定理6·18的系里的意义一致，$c_s=\varphi\left(p_s^{\alpha_s}\right)$ $(s=1,\cdots,k)$；若$(a,m)=1$，则$r,r_0,r_1,\cdots,r_k$，表示a对模m的一个指数组；$\rho,\rho_0,\rho_1,\cdots,\rho_k$；分别表示任一c次，$c_0$次，$c_1$次，…，$c_k$次单位根（因此各个ρ可能是复数）。

定义6·6 给定一组$\rho,\rho_0,\rho_1,\cdots,\rho_k$，则函数

$$\chi(a)=\begin{cases}\rho^{r}\rho_0^{r_0}\rho_1^{r_1}\cdots\rho_k^{r_k}, & (a,m)=1;\\ 0, & (a,m)>1.\end{cases}$$

叫做模m的一个特征函数(a characteristic function to modulus m)。

特别地，当$\rho=\rho_0=\rho_1=\cdots=\rho_k=1$时，对应的特征函数，叫做模m的主特征函数（principal characteristic function to modulus m)。

由定义6·6及定理6·21可以看出，特征函数是对所有整数a都有意义的单值函数。事实上，当$\gamma\equiv\gamma'(\bmod c),\gamma_i\equiv r_i'(\bmod c_i)\ (i=0,1,\cdots,k)$时，$\rho^{r}\rho_0^{r_0}\rho_1^{r_1}\cdots\rho_k^{r_k}=\rho^{r'}\rho_0^{r_0'}\rho_1^{r_1'}\cdots\rho_k^{r_k'}$.由假设共有c个ρ，$c_0$个$\rho_0$，$c_1$个$\rho_1$，…，$c_k$个$\rho_k$，所以共有$c\,c_0\,c_1\cdots c_k=\varphi(m)$组$\rho,\rho_0,\rho_1,\cdots,\rho_k$。因此有

定理6·24 对模m有φ(m)个不同的特征函数。

证明 由上面的分析，我们可以取φ(m)组不同的ρ，$\rho_0,\rho_1,\cdots,\rho_k$.因此对模m，最多有φ(m)个不同的特征函

数*。

今证明，若$(\rho, \rho_0, \rho_1, \cdots, \rho_k) \neq \left(\rho', \rho'_0, \rho'_1, \cdots, \rho'_k\right)$，则它们所对应的特征函数 $\chi(a) \neq \chi'(a)$。

因为$(\rho, \rho_0, \rho_1, \cdots, \rho_k) \neq (\rho', \rho'_0, \rho'_1, \cdots, \rho'_k)$，所以存在 s 使得$\rho_s \neq \rho'_s$。由定理6·22知，存在一个整数 a，使 a 对模 m 的指数组是：$r=0$，$r_0=0$，…，$r_s=1$，…，$r_k=0$。由定义6·6知

$$\chi(a)=\rho_s, \quad \chi'(a)=\rho'_s,$$

$$\therefore \quad \chi(a) \neq \chi'(a).$$

定理6·25 模 m 的特征函数$\chi(a)$有下列诸性质：

(i) $\chi(1)=1$； (a)

(ii) $\chi(a_1 a_2)=\chi(a_1)\chi(a_2)$；

(iii) 若$a_1 \equiv a_2 \pmod m$，则$\chi(a_1)=\chi(a_2)$。

证明 因为 1 对模 m 的指数组是 $r=0$，$r_0=0$，…，$r_k=0$，故

$$\chi(1)=\rho^0 \rho_0^0 \rho_1^0 \cdots \rho_k^0=1.$$

(ii) 设 a_1，a_2 的指数组分别是：

$r(a_1)$，$r_0(a_1)$，…，$r_k(a_1)$；$r(a_2)$，$r_0(a_2)$，…，$r_k(a_2)$。

则由定理6·23知，a_1a_2的指数组是：

$r(a_1)+r(a_2)$，$r_0(a_1)+r_0(a_2)$，…，$r_k(a_1)+r_k(a_2)$

---

* 两个特征函数不同，记作$\chi(a) \neq \chi'(a)$，指的是：存在一整数 a，使得函数值

$$\chi(a) \neq \chi'(a).$$

$\therefore\quad \chi(a_1a_2)=\rho^{r(a_1)+r(a_2)}\rho_0^{r_0(a_1)+r_0(a_2)}\cdots\rho_k^{r_k(a_1)+r_k(a_2)}$

$$=(\rho^{r(a_1)}\rho_0^{r_0(a_1)}\cdots\rho_k^{r_k(a_1)})\cdot$$

$$\cdot(\rho^{r(a_2)}\rho_0^{r_0(a_2)}\cdots\rho_k^{r_k(a_2)})=$$

$$=\chi(a_1)\cdot\chi(a_2).$$

(iii) 若$a_1\equiv a_2(\mathrm{mod}\ m)$，则$(a_1, m)=(a_2, m)$。当$(a_1, m)>1$时，$(a_2, m)>1$，故 $\chi(a_1)=\chi(a_2)=0$；当$(a_1, m)=1$时，$(a_2, m)=1$，由定理6·22知，a_1和a_2有相同的指数组，故$\chi(a_1)=\chi(a_2)$。

定义6·26

$$\sum_{a=0}^{m-1}\chi(a)=\begin{cases}\varphi(m), & \text{当}\chi(a)\text{是主特征函数时；}\\ 0, & \text{当}\chi(a)\text{不是主特征函数时。}\end{cases}$$

证明 (i) 当$\chi(a)$是主特征函数时，任给$(a, m)=1$，则$\chi(a)=1$，而0，1，…，$m-1$中与m互素的数共有$\varphi(m)$个，并且当$(a, m)>1$时$\chi(a)=0$所以

$$\sum_{a=0}^{m-1}\chi(a)=\varphi(m).$$

(ii) 当$\chi(a)$不是主特征函数时，由定义，有$\rho_s\neq1$，但$\rho_s^{c_s}-1=0$，即

$$(\rho_s-1)\left(\rho_s^{c_s-1}+\rho_s^{c_s-2}+\cdots+1\right)=0.$$

因此$\sum\limits_{\gamma_s=0}^{c_s-1}\rho_s^{r_s}=0$。故由定义得

$$\sum_{a=0}^{m-1}\chi(a)=\sum_{r=0}^{c-1}\sum_{r_0=0}^{c_0-1}\cdots\sum_{r_k=0}^{c_k-1}\rho^{r}\rho_0^{r_0}\cdots\rho_k^{r_k}$$

$$=\left(\sum_{r=0}^{c-1}\rho^{r}\right)\left(\sum_{r_0=0}^{c_0-1}\rho_0^{r_0}\right)\cdots\left(\sum_{r_k=0}^{c_k-1}\rho_k^{r_k}\right)=0.$$

定理6·27 若 a 是给定的一个整数，则

$$\sum_{\chi}\chi(a)=\begin{cases}\varphi(m)，若a\equiv1(\bmod m)；\\ 0，若a\not\equiv1(\bmod m)。\end{cases}$$

其中$\sum\limits_{\chi}$表示展布在$\varphi(m)$个特征函数上的和式。

证明 (i) 若$a\equiv1(\bmod m)$，则由定理6·25(i)知，对模 m 的每一个特征函数，都有$\chi(a)=1$。因此$\sum\limits_{\chi}\chi(a)=\varphi(m)$。

(ii) 若$a\not\equiv1(\bmod m)$，则由定义6·6知，当$(a, m)>1$时，对任一特征函数都有$\chi(a)=0$，故$\sum\limits_{\chi}\chi(a)=0$；当$(a,m)=1$时，则 a 有指数组 r，r_0，…，r_k，由定义6·6知

$$\sum_{\chi}\chi(a)=\left(\sum_{\rho}\rho^{r}\right)\left(\sum_{\rho_0}\rho_0^{r_0}\right)\cdots\left(\sum_{\rho_k}\rho_k^{r_k}\right).$$

其中 ρ 通过一切 c 次单位根，ρ_s 通过一切$c_s(s=0, 1, \cdots, k)$次单位根。

又因$a\not\equiv1(\bmod m)$，故 a 对模 m 的指数组中有一 r_s，适合 $c_s>r_s>0$，而$c_s>1$，今证对这个 s 来说，$\sum\limits_{\rho_s}\rho_s^{r_s}=0$。从高等代数中知道，对 c_s 来说有一c_s 次本原单位根 ε，使 $\varepsilon\neq1$（因为$c_s>1$），并且由于 $\varepsilon^{r_s}\neq1$，故有

$$\sum_{\rho_s}\rho_s^{r_s}=\sum_{r=0}^{c_s-1}(\varepsilon^{r})^{r_s}=\frac{1-(\varepsilon^{c_s})^{r_s}}{1-\varepsilon^{r_s}}=0.$$

于是$\sum\limits_{\chi}\chi(a)=0$。

定理6·28 设$\psi(a)$是定义在一切整数 a 上的复数值函数，则$\psi(a)$是模 m 的一个特征函数的充要条件是$\psi(a)$具有下列四个性质：

（i） 若$(a, m)>1$，则$\psi(a)=0$；

（ii） $\psi(a)$不恒等于0；

（iii） $\psi(a_1, a_2)=\psi(a_1)\psi(a_2)$；

（iv） 若$a_1\equiv a_2(\bmod m)$，则$\psi(a_1)=\psi(a_2)$.

证明 1. 必要性：若$\psi(a)$是模 m 的一个特征函数，则由定义6·6知(i)成立，又由定理6·25知性质(ii)、(iii)、(iv)成立。

2. 充分性：设$\psi(a)$是定义在一切整数 a 上且满足性质(i)—(iv)的函数，我们先证明

$$\psi(1)=1;\ 若(a, m)=1,\ 则\psi(a)\neq 0. \qquad (\alpha)$$

由性质(ii)知，$\exists a_1 \ni \psi(a_1)\neq 0$；由(iii)，$\psi(a_1)=\psi(a_1\cdot 1)=\psi(a_1)\psi(1)$，故$\psi(1)=1$.

由于$(a,m)=1$，故$\exists a' \ni a'a\equiv 1(\bmod m)$，由(iii)、(iv)及$\psi(1)=1$，即得$\psi(a)\psi(a')=\psi(aa')=\psi(1)=1$. 二复数之积为 1，此二复数必不为 0，所以当$(a, m)=1$时，$\psi(a)\neq 0$.

$\forall (a_1, m)=1$的a_1，由定理3·5的系 2 知，若 a 过模m的一个互素剩余系，则 a_1a 也过模 m 的一个互素剩余系，故由(iv)、(iii)及定理6·25得

$$\sum_a \frac{\chi(a)}{\psi(a)}=\sum_a \frac{\chi(a_1a)}{\psi(a_1a)}=\frac{\chi(a_1)}{\psi(a_1)}\sum_a \frac{\chi(a)}{\psi(a)},$$

其中$\chi(a)$是对模 m 的任一特征函数；$\sum\limits_a$表示展布在 a 所通过的互素剩余系的一切整数上的和式，由此即得

$$\sum_{a}\frac{\chi(a)}{\psi(a)}\left(1-\frac{\chi(a_1)}{\psi(a_1)}\right)=0,$$

此等式对给定的特征函数$\chi(a)$来说，必有

$$\sum_{a}\frac{\chi(a)}{\psi(a)}=0,\ \text{或者}\quad \chi(a_1)=\psi(a_1)$$

之一成立。要证对一切$(a_1, m)=1$的a_1后一式都成立。只要证明，有一个特征函数$\chi(a)$使得前一个等式不成立，就可以了。

假定对于每一个特征函数$\chi(a)$来说，都有

$$\sum_{a}\frac{\chi(a)}{\psi(a)}=0,$$

则

$$H=\sum_{\chi}\sum_{a}\frac{\chi(a)}{\psi(a)}=0, \tag{β}$$

其中χ通过模m的一切特征函数。另一方面，由定理6·27及(α)知，$\forall(a, m)=1$的a，都有

$$\sum_{\chi}\frac{\chi(a)}{\psi(a)}=\frac{1}{\psi(a)}\sum_{\chi}\chi(a)$$

$$=\begin{cases}\dfrac{1}{\psi(a)}\cdot\varphi(m) & \text{若}a\equiv1\pmod m;\\ 0 & \text{若}a\not\equiv1\pmod m.\end{cases}$$

由于模m的互素剩余系中，有且只有一个数$a\equiv1\pmod m$，所以

$$H=\sum_{a}\sum_{\chi}\frac{\chi(a)}{\psi(a)}=\frac{1}{\psi(a)}\varphi(m)\neq0,$$

这与(β)矛盾。因此有一特征函数$\chi(a)$存在，使得$\sum\frac{\chi(a)}{\psi(a)}$

$\neq 0$。且若$(a, m)=1$，则$\psi(a)=\chi(a)\neq 0$，故这个特征函数$\chi(a)$与$\psi(a)$相同，即$\psi(a)$是一个特征函数。即$\exists\chi(a)\ni\chi(a)=\psi(a)$。

这个定理与定义6·6等价，下面举几个特征函数的例子。

例6·14 设p是奇素数，则对模p的勒让得符号是对模p的一个特征函数。这个结论可由勒让得符号的性质，直接得到。

例6·15 设p是大于1的奇数，则对模p的雅可比符号，是对模p的一个特征函数。

习　题

1. 求所有与m互素的数，对于模m所属的方次数，当(i) $m=5$，(ii) $m=8$，(iii) $m=10$，(iv) $m=11$，(v) $m=24$时。

2. 设p是奇素数，整数$a>1$，证明：

(i) a^p-1的奇素因数是$a-1$的因数，或是形如$2px+1$的整数，其中x是正整数。

(ii) a^p+1的奇素因数是$a+1$的因数，或是形如$2px+1$的整数，其中x是正整数。

3. 证明形如$2px+1$的素数的个数是无穷的。

4. 设n为正整数，证明$2^{2^n}+1$有形如$2^{n+1}x+1$的约数，其中x是正整数。

5. 设整数$a>1$，$n>0$。证明$n\mid\varphi(a^n-1)$。

6. 若$a\in_m\delta$，则$a^\lambda\in_m\dfrac{\delta}{(\lambda, \delta)}$。

7. 求出下列数的所有原根：(i)7；(ii)17；(iii)49；(iv)125；(v)81；(vi)14；(vii)50。

8. 引用第四章习题8的记号，分数$\dfrac{b}{a}$(mod m)即同余式$ax\equiv b$(mod m)的解。特别，当$a\mid b$时，$\dfrac{b}{a}$即通常的商数。证明：$\dfrac{b}{a}$对模

m 的指数，等于分子和分母指数之差，即$\text{ind}\frac{b}{a}=\text{ind}\,b-\text{ind}\,a$。

9. 证明-1（即$m-1$）的指数与$\frac{1}{2}\varphi(m)$关于模$\varphi(m)$同余。

10. 除$m=2$外，模 m 的原根都是模 m 的平方非剩余。

11. 对序列

$$1,\ 2,\ \cdots,\ n\ (n>1) \tag{a}$$

施行如下的 k 次运算：

(i) 当 n 是奇数时：

$$1,\ 3,\ 5,\ \cdots,\ n-2,\ n,\ n-1,\ n-3,\ \cdots,\ 4,\ 2; \tag{a_1}$$

$$1,\ 5,\ 9,\ \cdots,\ 11,\ 7,\ 3; \tag{a_2}$$

…… …… …… ……;

$$1,\ 2,\ 3,\ \cdots,\ n. \tag{a_k}$$

(ii) 当 n 是偶数时：

$$1,\ 3,\ 5,\ \cdots,\ n-1,\ n,\ n-2,\ \cdots,\ 4,\ 2; \tag{a_1'}$$

$$1,\ 5,\ 9,\ \cdots,\ 11,\ 7,\ 3; \tag{a_2'}$$

…… …… …… ……;

$$1,\ 2,\ 3,\ \cdots,\ n. \tag{a_k'}$$

证明，这样 k 次运算后给出原先的序列[$(a)=(a_k)$或$(a)=(a_k')$]的充要条件是$2^k\equiv\pm1 \pmod{2n-1}$。

12. 设整数$n>1$，$m>1$作序列

$$1,\ 2,\ \cdots,\ n,\ n,\ n-1,\ \cdots,\ 2;\ 1,\ 2,\ \cdots,\ n,\ n,\ \cdots,\ 2;\ 1,\ 2,\ \cdots. \tag{b}$$

在(b)中取出第 1，$m+1$，$2m+1$，…，$(n-1)m+1$的数，依次排列成 n 个数目的新序列(a_1)，把(a_1)再按上述方法（形式如(b)的排法）排出序列(c)，再对(c)施行同样的运算，继续下去．证明，第 k 次运算后给出原先的序列(a)（与11题同）的充要条件是：

$$m^k\equiv\pm1 \pmod{2n-1}$$

13. 设q_1，q_2，…，q_k是$\varphi(m)=c$的一切素因数，证明，g 是模 m 的一个原根的充要条件是：g 是模 m 的 q_i 次非剩余。

14. (i) 证明 3 是形如 2^n+1，$n>1$的素数的原根。

(ii) 证明，形如 $2p+1$的素数，当 p 是 $4n+1$ 形式时，有原根 2；当 p 是 $4n+3$时，有原根 -2。

(iii) 证明，2 是 $4p+1$形素数的原根。

(iv) 证明，3 是下列素数的原根：

$2^n p+1$，其中 $n>1$，$p>\frac{3^{2^{n-1}}}{2^n}$ $(p\neq 3)$。

15. 证明，10是模17及模257(素数)的原根，并用以证明把$\frac{1}{17}$，$\frac{1}{257}$化成循环小数时，循环节的长度分别是16及256。

16. 借指数的帮助，解下诸同余式：

(i) $x^2\equiv 59 \pmod{83}$；　(ii) $x^2\equiv 32 \pmod{43}$；

(iii) $x^2\equiv -17 \pmod{53}$；　(iv) $18x\equiv 42 \pmod{89}$

(v) $35x+15\equiv 0 \pmod{97}$；　(vi) $x^8\equiv 15 \pmod{41}$；

(vii) $x^5\equiv 17 \pmod{29}$；　(viii) $x^7\equiv 3 \pmod{61}$；

(ix) $x^8\equiv 22 \pmod{43}$；　(x) $x^6\equiv 15 \pmod{53}$；

(xi) $x^4\equiv 11 \pmod{59}$；　(xii) $5x\equiv 13 \pmod{27}$；

(xiii) $x^2\equiv 10 \pmod{27}$。

第七章 代数整数

本章将初步讨论代数数和超越数，并借助代数数的性质具体地找出一些超越数，证明最常用的超越数 e（自然对数的底）和 π（圆周率）的超越性。此外，还将讨论在有理整数有哪些性质在代数整数集中被保持，哪些性质被破坏，特别是研究算术基本定理的存在条件，使我们对整数的性质有进一步了解。

第一节 代数数与超越数

全体复数可以分为代数数和超越数两类。

定义7·1 若复数 ξ 是一个有理系数多项式

$$f(x)=x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n \qquad (1)$$

的根，则称 ξ 是一个代数数（algebric number）。若$f(x)$的系数 a_1，a_2，…，a_n 都是有理整数，则称 ξ 是一个代数整数（algebraic integer）。

若 ξ 所满足的最低次数的多项式$f(x)$的次数是 n，则 n 称为 ξ 的次数，这时，ξ 称为 n 次代数数（n 次代数整数）。

例如，$i=\sqrt{-1}$，$\omega=\frac{1}{2}(-1+\sqrt{-3})$分别是 x^2+1，x^2+x+1 的根，则 i 和ω都是二次代数数，并且都是二次代数整数（简称二次整数）。

又 $\rho=\frac{1+\sqrt{5}}{4}$是 $x^2-\frac{1}{2}x-\frac{1}{4}$的根，所以$\rho$是一个二

次代数数，但不是二次整数。

定理7·1 每一个代数数都满足一个首项系数是1的有理系数不可约多项式，并且这样的多项式是唯一的。若这个代数数是整数，则上述多项式的首项系数是1，其他系数都是有理整数。

下面如无特别声明，都用∂f表示多项式$f(x)$的次数；K表示有理数域；R表示有理整数环。

证明 (i) 因为任一代数数ξ，都是某些首项系数为1的有理系数多项式的根，故其中必有一个次数最低的多项式$f(x)$，设$\partial f=n$，则

$$f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_n,\quad a_i\in K$$

这样的$f(x)$必不可约。否则$f(x)=f_1(x)f_2(x)$，而且$\partial f_1<n$，$\partial f_2<n$，于是由$f(\xi)=0$可知，$f_1(\xi)=0$或$f_2(\xi)=0$这与∂f的最小性矛盾。

若$g(\xi)=0$，$g(x)=x^m+b_1x^{m-1}+\cdots+b_n$，$b_i\in K$。由带余除法，得

$$g(x)=f(x)q(x)+r(x),\quad \partial r<\partial f$$

以$x=\xi$代入上式，得

$$g(\xi)=f(\xi)q(\xi)+r(\xi)\Longrightarrow r(\xi)=0.$$

由于∂f的最小性，因而$r(x)=0$，即

$$g(x)=f(x)q(x),\quad \partial g\geqslant\partial f$$

但若$g(x)$亦首项系数为1的不可约多项式，则$q(x)=1$，即

$$g(x)=f(x)$$

这就证明了唯一性。

(ii) 在高等代数里我们知道，若$a_i\in R$（$i=0,1,\cdots,n$），且$(a_0,a_1,\cdots,a_n)=1$，则称多项式

$$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n$$

为本原多项式（primitive polynomial）。并且还证明了：两个本原多项式之积仍为本原多项式；任一有理系数多项式

$$\varphi(x)=\frac{a_0}{b_0}x^n+\frac{a_1}{b_1}x^{n-1}+\cdots+\frac{a_n}{b_n}=\frac{a}{b}\psi(x).$$

其中 a_i，b_i，a、$b\in R$，$(a_0, a_1, \cdots, a_n)=a$，$(b_0, b_1, \cdots, b_n)=b$，$\psi(x)$是本原多项式，且$\psi(x)$是唯一确定的。

设ξ是一个代数整数，由定义7·1 知，ξ是 R 上不可约多项式

$$F(x)=x^m+a_1x^{m-1}+\cdots+a_m,\quad a_i\in R(i=1, \cdots, n)$$

的根。若$F(x)$在有理数域K上可约，则

$$F(x)=f(x)q(x)\ (\partial f<m)$$

用上述高等代数的知识可知，存在本原多项式$f^*(x)$和$q^*(x)$，使得

$$f(x)=\frac{a}{b}f^*(x),\quad q(x)=\frac{c}{d}q^*(x)$$

$$\Longrightarrow F(x)=\frac{ac}{bd}f^*(x)q^*(x)=\frac{ac}{bd}F^*(x)$$

其中$F^*(x)$亦本原多项式。由于有理系数多项式表示成本原多项式是唯一的，故

$$F(x)=F^*(x)=f^*(x)q^*(x)\quad(\partial f^*=\partial f<m)$$

其中 $f^*(x)$和 $g^*(x)$都是首项系数为 1 的本原多项式，这与$F(x)$在 R 上不可约的假设矛盾。

系 有理数 a 是代数整数的充要条件是：a 为有理整数。

证明 因为R上多项式

$$f(x)=a_0x^n+\cdots+a_{n-1}x+a_n$$

的任一有理根 $a=\frac{c}{d}$，当$(c, d)=1$时，都有 $c|a_n$，$d|a_0$。

若 a 是代数整数，$f(a)=0$，则由定义7·1知，$a_0=1$，故 $d=1$，从而 $a=c$ 为有理整数。

反之，若 a 是有理整数，则 a 是 $x-a$ 的根，因而 a 是代数整数。

定理7·2 所有代数数的集合A，是复数域C的子域。

证明 只要证明任意二代数数的和、差、积、商仍为代数数，就可以了。

设 α、β 分别是 n 次，m 次代数数，即它们分别满足 K 上不可约多项式

$$f(x)=x^m+a_1x^{m-1}+\cdots+a_m$$

$$g(x)=x^m+b_1x^{m-1}+\cdots+b_m$$

设其复数根分别为 $\alpha=\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n$；$\beta=\beta_1,\ \beta_2,\ \cdots,\ \beta_m$*。构造多项式

$$\varphi(x)=\prod_{i=1}^{n}\prod_{j=1}^{m}[x-(\alpha_i+\beta_i)]。$$

显然 $\varphi(x)$的右边，对于 α_i 经任意置换，β_j 经任意置换后不变，即 $\varphi(x)$的各项系数都不变。所以系数都是 α_1、α_2、…、α_n 和 β_1、β_2、…、β_m 的对称多项式，根据高等代数中两组不定元对称多项式的基本定理**知，它们都是f(x)，

---

* $\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n$，叫做α的共轭数；$\beta_1,\ \beta_2,\ \cdots,\ \beta_m$叫做β的共轭数。

** 域P上关于两组不定元 $\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n$ 和 $\beta_1,\ \beta_2,\ \cdots,\ \beta_m$ 对称的任一多项式，都可以表为这两组不定元的初级对称多项式

$\sigma_1=\alpha_1+\alpha_2+\cdots+\alpha_n$，　　$\sigma_1'=\beta_1+\beta_2+\cdots+\beta_m$

$\sigma_2=\alpha_1\alpha_2+\alpha_1\alpha_3+\cdots+\alpha_{n-1}\alpha_n$，　　$\sigma_2'=\beta_1\beta_2+\beta_1\beta_3+\cdots+\beta_{m-1}\beta_m$，

………，　　………，

$\sigma_m=\alpha_1\alpha_2\cdots\alpha_n$；　　$\sigma_m'=\beta_1\beta_2\cdots\beta_m$。

的多项式，若把$\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n$；$\beta_1,\ \beta_2,\ \cdots,\ \beta_m$看作是f(x)，g(x)的根时，则$\sigma_i=(-1)^ia_i(i=1,\ 2,\ \cdots,\ n)$，$\sigma_j'=(-1)^jb_j(j=1,\ 2,\ \cdots,\ m)$。

$g(x)$的系数的多项式。也就是$\varphi(x)$的系数都是有 理数，且首项系数是1，因而它的根 $\alpha+\beta=\alpha_1+\beta_1$ 是一个代数数。

同样地，借助于多项式

$$\psi(x)=\prod_{i=1}^{n}\prod_{j=1}^{m}[x-(\alpha_i-\beta_j)]$$

与

$$\theta(x)=\prod_{i=1}^{n}\prod_{j=1}^{m}(x-\alpha_i\beta_j)$$

可以证明 $\alpha-\beta$ 与 $\alpha\beta$ 亦都是代数数。

为了证明商是一个代数数，只要证明，若 $\alpha\neq 0$ 是一个代数数，则 $\alpha^{-1}=\frac{1}{\alpha}$亦必为代数数就可以了。设 α 是有 理系数多项式

$$f(x)=x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n \quad (a_n\neq 0)$$

的根，显然，α^{-1}是

$$\begin{aligned}g(x)&=a_ny^n+a_{n-1}y^{n-1}+\cdots+a_1y+1\\&=a_n\left(y^n+\frac{a_{n-1}}{a_n}y^{n-1}+\cdots+\frac{a_1}{a_n}y+\frac{1}{a_n}\right)\\&=a_n(y^n+b_1y^{n-1}+\cdots+b_{n-1}y+b_n)\end{aligned}$$

的根，故 α^{-1}亦是代数数。

由于任一代数数都是复数，故$A\subset C$。

系 一切代数整数的集合 I 是A 的子环。

只需证明任意两个代数整数的和、差、积仍为代数整数就可以了。其证法与定理7·2一致。

定理7·3 以代数数为系数的多项式的根，也是代数数。

证明 设 ω 是系数为代数数的多项式

$$\varphi(x)=x^n+\alpha x^{n-1}+\beta x^{n-2}+\cdots+\lambda x+\mu$$

的根。设 $\alpha=\alpha_1$，α_2，…，α_k；$\beta=\beta_1$，β_2，…，β_l；…，

$\lambda=\lambda_1, \lambda_2, \cdots, \lambda_m$; $\mu=\mu_1, \mu_2, \cdots, \mu_g$是它们的共轭数，构造

$$F(x)=\prod_{i,j,\cdots s,t}\varphi_{i,j,\cdots,s,t}(x)$$

其中$i=1, 2, \cdots, k$; $j=1, 2, \cdots, l$; $\cdots s=1, 2, \cdots, m$; $t=1, 2, \cdots, q$。上式右边是$\varphi(x)$的系数取$\alpha, \beta, \cdots, \lambda, \mu$一切可能的共轭数所构成的$k\cdot l\cdots m\cdot q$个$n$次多项式之积，其中$\varphi_{1,1,\cdots,1,1}(x)=\varphi(x)$。

显然$F(x)$的系数对每一组共轭数$\alpha_i, \beta_j, \cdots, \lambda_s, \mu_t$都是对称的，故$F(x)$的系数都是有理数。事实上，$F(x)$是以$\alpha, \beta, \cdots, \lambda, \mu$所满足的有理系数多项式的系数为系数的多项式，所以$F(x)$的系数亦是有理数。而$F(\omega)=0$，因而$\omega$是代数数。

由这个定理知道，一串以代数数为系数的多项式的根仍是代数数。例如，

$$\omega=\sqrt[3]{1+\sqrt{1+\sqrt{2}}}$$

是如下的一串以代数数为系数的多项式的最后一个多项式的根。

$$x^2-2,\ y^2-(1+\sqrt{2}),\ z^3-(1+\sqrt{1+\sqrt{2}}) \qquad (2)$$

事实上，$\sqrt{2}$是(2)的第一个多项式的根，把它添加于有理数域K，得到$K(\sqrt{2})$*。所以第二个多项式是$K(\sqrt{2})$

* $k(\sqrt{2})$指的是：一切有理数a, b, c与$\sqrt{2}$，经过实数的加、减、乘、除（0不作除数）四种运算所得到的一切实数的集合。其中任一数都可表成$a+b\sqrt{2}$，$a, b\in k$，的形式，并且一切形如$a+b\sqrt{2}$（$a, b\in k$）的数都属于$k(\sqrt{2})$，通常称$k(\sqrt{2})$为k上的一个二次有限扩张（quadratic finite extension）。容易证明，$k(\sqrt{2})$是实数域的一个子域。

$k(\sqrt{2})$上的多项式，指的是系数都属于$k(\sqrt{2})$的多项式。

上的多项式，把它的根再添加于$K(\sqrt{2})$，得到$K(\sqrt{2})(\sqrt{1+\sqrt{2}})=K(\sqrt{2},\sqrt{1+\sqrt{2}})$，是$K(\sqrt{2})$上的一个二次有限扩张。$(1+\sqrt{1+\sqrt{2}})\in K(\sqrt{2},\sqrt{1+\sqrt{2}})$，所以(2)的第三个多项式是$K(\sqrt{2},\sqrt{1+\sqrt{2}})$上的一个多项式。

定义7·2 若一个数域的一切数都是代数数，则称这个数域为代数数域（field of algebraic numbers）。每一个数都是代数整数的数环，称为代数整数环（ring of algebraic integers）。

如，有理数域K，$K(\sqrt{2})$，$K(\sqrt{2},\sqrt{1+\sqrt{2}})$，$K(i)$ $(i=\sqrt{-1})$等都是代数数域。有理整数环R，$R[\sqrt{2}]$ $R[\sqrt{5}]$，$R[i]$，$R[\sqrt{2},\sqrt{1+\sqrt{2}}]$*以及一切代数整数的集合I等，都是代数整数环。

定理7·4 若ξ是一个二次代数数，则$K(\xi)$是一个代数数域。并且存在一个不含平方因数的非零有理整数m，使得$K(\xi)=K(\sqrt{m})$。即$K(\xi)$是由一切形如

$$a+b\sqrt{m},\quad a,\ b\in K$$

的数所组成。

证明：(i) 因为ξ是一个二次代数数，所以ξ是不可

---

* $R[\sqrt{2}]$指的是：一切有理整数a、b、c与$\sqrt{2}$经过实数的加、减、乘三种运算所得到的一切实数的集合。它包含一切形如$a+b\sqrt{2}$的集合，其中a、a$\in$K，它是$K(\sqrt{2})$的子环。同样地$R[i]$和$R[\sqrt{2},\sqrt{1+\sqrt{2}}]$是$R(i)$和$R(\sqrt{2},\sqrt{1+\sqrt{2}})$的子环，并且它们的每一个元素都是代数整数。而$R[\sqrt{5}]$都是任意形如$a+b\omega$ $(\omega=\frac{1}{2}(\sqrt{5}-1))$，a，b$\in$R，的代数整数的集合，它也是一个数环。

并注意$K(\sqrt{m})$有添加$\sqrt{m}$于K的意义；而$R[\sqrt{m}]$无“添加”的意义。

约的有理系数二次多项式

$$x^2+a_1x+a_2,\quad a_1,\ a_2\in K$$

的根。由二次方程解的公式，知道

$$\xi=\frac{1}{2}(-a_1+\sqrt{\Delta}),\Delta=a_1^2-4a_2\in K$$

Δ 不是完全平方的有理数，故存在 r，$s\in R$，$s>0$，使得

$$\Delta=\frac{r}{s}\Longrightarrow\sqrt{\Delta}=\frac{1}{s}\sqrt{rs}=\frac{t}{s}\sqrt{m}\neq 0$$

其中 s，t，$m\in R$，m 不含有理整数平方因子的非零有理整数，所以

$$K(\xi)=K\left(\frac{1}{2}(-a_1+\sqrt{\Delta})\right)=K(\sqrt{\Delta})=K(\frac{t}{s}\sqrt{m})$$
$$=K(\sqrt{m})$$

(ii) 任给

$$f(x)=x^n+c_1x^{n-1}+\cdots+c_n,\quad c_i\in K$$

由带余除法，得

$$f(x)=(x^2-m)q(x)+bx+a,\quad a,\ b\in K$$
$$\Longrightarrow f(\sqrt{m})=a+b\sqrt{m}$$

这说明了，任意有理数与$\sqrt{m}$的加、减、乘运算的结果，都是形如 $a+b\sqrt{m}$ ($a,\ b\in K$)的数，并且 $a+b\sqrt{m}$ 是

$$k(x)=x^2-2ax+a^2-b^2m \tag{3}$$

的根，所以 $a+b\sqrt{m}$ 是一个代数数。

(iii) 最后，设 $g=a_1+b_1\sqrt{m}$，$h=a_2+b_2\sqrt{m}\neq 0$，则

$$r=\frac{g}{h}=\frac{a_1+b_1\sqrt{m}}{a_2+b_2\sqrt{m}}$$
$$=\frac{a_1a_2-b_1b_2m}{a_2^2-b_2^2m}+\frac{a_2b_1-a_1b_2}{a_2^2-b_2^2m}\sqrt{m}$$
$$=A+B\sqrt{m}\quad (A,\ B\in K)$$

故 $r\in K(\sqrt{m})$，并且 r 是 $x^2-2Ax+A^2-B^2m$ 的根，所以 $K(\sqrt{m})$ 是一个代数数域。

定义7·3 若 ξ 是一个二次代数数，则 $K(\xi)$ 叫做二次数域（field of quadratic numbers）

从定理7·4知道，任一二次数域都是 $K(\sqrt{m})=\{x|a+b\sqrt{m}\}$ 形的集合，其中 m 是不含平方因子的非零有理整数，a，$b\in K$，并且从定理7·4的证明过程中知道，$K(\sqrt{m})$ 中任一非有理数的数都是二次代数数。

定理7·5 若 m 是不含平方因数的有理整数，则 $K(\sqrt{m})$ 中的一切代数整数可以表成

$$a+b\omega,\ a,\ b\in R,\omega=\begin{cases}\sqrt{m}, & \text{当}m\not\equiv 1\ (\text{mod }4)\\ \frac{1}{2}(\sqrt{m}-1), & \text{当}\equiv 1\ (\text{mod }4)\end{cases} \tag{4}$$

形式

证明 任给 $\xi=a+b\sqrt{m}$，$\xi\in K(\sqrt{m})$、由定理7·4知 ξ 是(3)的根，所以 ξ 是代数整数的充要条件是：$2a$ 及 a^2-b^2m 都是有理整数。

令 $2a=A$，$a^2-b^2m=C$，则 A，$C\in R$ 是 ξ 为代数整数的充要条件．因为 $b\in K$，所以 $2b\in K$，设 $2b=\frac{r}{s}(s>0)$，r，$s\in R$，$(r,\ s)=1$。若 A，$C\in R$，则 $(2b)^2m=A^2-4C\in R\Longrightarrow s^2|r^2m\xrightarrow{(s^2,\ r^2)=1}s^2|m\Longrightarrow s=1$。

$\therefore\quad 2b=r\in R$

令 $2b=B$，$B\in R$，且

$$B^2m=A^2-4C\Longrightarrow\frac{1}{4}(A^2-B^2m)=C\in R$$

由于上面的讨论，条件"A，$C\in R$"便转化为：

"$a=\frac{A}{2}$, $b=\frac{B}{2}$, $A,B\in R$ 且 $A^2-B^2m\equiv0\pmod 4$" 即是说，$\xi=a+b\sqrt{m}$ 是代数整数的充分必要条件是 $\xi=\frac{1}{2}(A+B\sqrt{m})$，$A,B\in R$，且 $A^2-B^2m\equiv0\pmod4$ （5）

下面证明A与B不能是一奇一偶的。

因为 $4\mid A^2-B^2m$，若 $A=2k$，$B=2k+1$，则

$A^2-B^2m\equiv-m\equiv0\pmod 4\Longrightarrow4\mid m$

这与 m 不含平方因子的假设矛盾。若 $A=2k+1$，$B=2h$，则 $A^2-B^2m\equiv1\pmod4$，这是不可能的。所以A和B只能是同为奇数，或同为偶数。

(i) 当 $m\not\equiv1\pmod 4$ 时，A与B不能同时是奇数。否则，$A^2\equiv1$，$B^2\equiv1\pmod 4$，因而

$0\equiv A^2-B^2m\equiv1-m\pmod4\Longrightarrow m\equiv1\pmod 4$

与假设矛盾。故此时A，B必须同为偶数。由（5）知 $\xi=a+b\sqrt{m}$ 为代数整数的充要条件是：a，$b\in R$ 即（4）中 $\omega=\sqrt{m}$。

(ii) 当 $m\equiv1\pmod 4$ 时，不论A，B同是奇数或者同是偶数，总有

$$A^2-B^2m\equiv A^2-B^2\equiv0\pmod 4$$

$$\Longrightarrow\frac{1}{4}(A^2-B^2m)=C\in R,$$

由（5）知 $\xi=a+b\sqrt{m}$ 为代数整数的充要条件是：

$$\xi=\frac{1}{2}(A+B\sqrt{m})$$

其中A，B同为奇数或同为偶数。此时

$$\xi=\frac{1}{2}(A+B)+\frac{1}{2}B(\sqrt{m}-1)=\frac{A+B}{2}+B\omega,$$

$\omega = \frac{1}{2}(\sqrt{m}-1)$其中：$\frac{A+B}{2}$，$B \in R$。

任给 a，$b \in R$，令$\frac{A+B}{2} = a$，$B = b$则$A = 2a - b$，$B = b$，故A、B必同为奇数或同为偶数。所以$K(\sqrt{m})$中的一切代数整数，都可以表成

$$a + b\omega,\quad \omega = \frac{1}{2}(\sqrt{m} - 1)$$

的形式，其中 a、b是任意有理整数。

定理7·5中所给出的代数整数的集合，记作$R[\sqrt{m}]$。

例如，$K(i)$内的一切代数整数都是形如$a+bi$（a，$b \in R$）的复数，即

$$R[i] = \{a + bi \mid a,\ b \in R\}$$

$$R[\sqrt{-3}] = \{a + \frac{b}{2}(\sqrt{-3} - 1) \mid a, b \in R\}$$

$$R[5] = \{a + \frac{b}{2}(\sqrt{5} - 1) \mid a,\ b \in R\}$$等等

系 $R[\sqrt{m}]$是一个数环（代数整数环）。

证明 任给ξ，$\eta \in R[\sqrt{m}]$，则由定理7·5知

$\xi = a_1 + b_1\omega$，$\eta = a_2 + b_2\omega$，a_1，b_1，a_2，$b_2 \in R$

$$\omega = \begin{cases} \sqrt{m}, & 当\ m \not\equiv 1 \pmod 4; \\ \frac{1}{2}(\sqrt{m} - 1), & 当\ m \equiv 1 \pmod 4. \end{cases}$$

显然，$\xi \pm \eta = (a_1 \pm a_2) + (b_1 \pm b_2)\omega \in R[\sqrt{m}]$

$$\because \quad \omega^2 = \begin{cases} m, & 当 m \not\equiv 1 \pmod 4 \\ \frac{m-1}{4} - \omega, & 当 m \equiv 1 \pmod 4 \end{cases}$$

$$\therefore\quad \xi\eta=\begin{cases}(a_1a_2+b_1b_2m)+(a_1b_2+a_2b_1)\omega, & \text{当} m\not\equiv 1(\mathrm{mod}4)\\ (a_1a_2+\dfrac{m-1}{4}b_1b_2)+(a_1b_2+a_2b_1-b_1b_2)\omega, & \text{当} m\equiv 1(\mathrm{mod}4)\end{cases}$$

故 $\xi\eta\in R[\sqrt{m}]$。这就证明了 $R[\sqrt{m}]$是一个数环。

定义7·4 不是代数数的复数，叫做超越数（transcendental number）。也就是，超越数不是任何有理系数多项式的根。

自然对数的底 e 和圆周率 π 是两个著名的超越数，本章后面将给出此事的一种证法，下面先介绍一种具体构造超越数的方法。

定理7·6 若 ξ 是一个实 n（$n>1$）次代数数，则只能找到有限个有理数$\frac{p}{q}$，满足

$$\left|\xi-\frac{p}{q}\right|\leqslant\frac{1}{q^{n+1}},\quad q>0 \tag{6}$$

要证明本定理，只要证明满足（6）的 q只有有限个，且对于确定的 q，p 也只有有限个，就可以了．

证明 因为 ξ 是一个实 n 次代数数，故 ξ 是一个 n次不可约的整系数多项式：

$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n$，$a_0\neq0$，$a_i\in R(i=0,1,\cdots,n)$的根．设 $\xi_1,\cdots,\xi_{n-1}$ 是 f(x) 的其他 n−1个根，显然 $\xi_i\neq\xi$（$i=1,\cdots,n-1$）．否则，f(x) 有重根，但重根的共轭数亦为 f(x)的重根，这样 f(x)就变成可约的了．

令

$\min(|\xi_1-\xi|, \cdots, |\xi_{n-1}-\xi|, 1)=\rho$，则$1\geqslant\rho>0$。

(i) 若有理数$\frac{p}{q}(q>0)$，满足

$$\frac{1}{q^{n+1}}\geqslant\left|\xi-\frac{p}{q}\right|\geqslant\rho$$

$$\Longrightarrow q\leqslant\frac{1}{\sqrt[n+1]{\rho}}<\left[\frac{1}{\sqrt[n+1]{\rho}}\right]+1$$

由于$[1/\sqrt[n+1]{\rho}]$是一个确定的正有理整数，故只有有限个正有理整数q满足不等式(6)。

若给定q，则由不等式

$$\left|\xi-\frac{p}{q}\right|\leqslant\frac{1}{q^{n+1}}$$

得
$$-\frac{1}{q^{n+1}}\leqslant\xi-\frac{p}{q}\leqslant\frac{1}{q^{n+1}}$$

即
$$-q\xi-\frac{1}{q^n}\leqslant-p\leqslant-q\xi+\frac{1}{q^n}$$

亦即
$$q\xi+\frac{1}{q^n}\geqslant p\geqslant q\xi-\frac{1}{q^n}$$

所以只有有限个有理整数p满足上面不等式，亦即满足不等式(6)的p只有有限个。

(ii) 若$0<\left|\xi-\frac{p}{q}\right|<\rho$，$q>0$，则

$$-\rho<\frac{p}{q}-\xi<\rho\Longrightarrow\xi-\rho<\frac{p}{q}<\xi+\rho\Longrightarrow f\left(\frac{p}{q}\right)\neq0$$

$$\therefore\quad \left|f\left(\frac{p}{q}\right)\right|=\frac{|a_0p^n+a_1p^{n-1}q+\cdots+a_nq^n|}{q^n}\geqslant\frac{1}{q^n}\qquad(7)$$

又由拉格朗日中值定理，知

$$f\left(\frac{p}{q}\right)=f\left(\frac{p}{q}\right)-f(\xi)=\left(\frac{p}{q}-\xi\right)f'(x)\qquad(8)$$

其中x在$\frac{p}{q}$及ξ之间，且$f'(x)\neq0$。设

$$M=\max_{\xi-\rho\leqslant x\leqslant\xi+\rho}|f'(x)|$$

则由(7)与(8)即得

$$\left|\xi-\frac{p}{q}\right|=\left|\frac{p}{q}-\xi\right|=\frac{\left|f\left(\frac{p}{q}\right)\right|}{|f'(x)|}\geqslant\frac{1}{Mq^{n}}$$

由(6)得

$$\frac{1}{q^{n+1}}\geqslant\frac{1}{Mq^{n}}\Longrightarrow M\geqslant q$$

故只有有限个有理整数 q 满足不等式(6)。与(i)同样地证明，对于给定的 q，只有有限个有理整数 p 满足(6)。

定理7·6提供了一个具体构造超越数的方法，因为这个定理的逆否命题是：“如果实数 α，对于每一个自然数 n 都有无限多个有理数 $\frac{p}{q}$ 满足不等式(6)，那末 α 是一个超越数。”要使对于每一个 n 都有无限多个有理数满足(6)，我们只要寻找一个实数使得能用一个有理数列迅速地趋近它（余项充分小），这时这个实数就是超越数。

例7·1 $\xi=\sum_{n=1}^{\infty}\frac{1}{10^{n!}}$是一个超越数。

证明 令

$$\sum_{k=1}^{n}\frac{1}{10^{n!}}=\frac{p_n}{q_n}\in K$$

对于任一自然数N，当n>N时

$$0<\xi-\frac{p_n}{q_n}=\sum_{k=n+1}^{\infty}\frac{1}{10^{k!}}=\frac{1}{10^{(n+1)!}}+\frac{1}{10^{(n+2)!}}+\cdots$$

$$<\frac{1}{10^{(n+1)!}}+\frac{1}{10^{(n+1)!}}\cdot\frac{1}{2}$$

$$+\frac{1}{10^{(n+1)!}}\cdot\frac{1}{2^{2}}+\cdots$$

$$= \frac{1}{10^{(n+1)!}}\left(1+\frac{1}{2}+\frac{1}{2^2}+\cdots\right)=\frac{2}{10^{(n+1)!}}$$

$$= \frac{2}{q_n^{n+1}} < \frac{1}{q_n^{N+1}}$$

由于大于N的自然数有无限多个，故有无限多个$\frac{p_n}{q_n}$$(n>N)$存在，使得

$$\left|\xi-\frac{p_n}{q_n}\right|<\frac{1}{q_n^{N+1}}$$

于是由定理7·6的逆否命题知道，ξ不是N次代数数。由于N的任意性，所以ξ是超越数。

一般地

$$\xi=\sum_{n=1}^{\infty}\frac{a_n}{10^{n!}},\quad 0\leqslant a_n\leqslant 9\ (n=1,\ 2,\ \cdots)$$

当只有有限个$a_n\neq 0$时，ξ是有理数，而有无限多个$a_n\neq 0$时，ξ是无理数．后者令

$$\sum_{k=1}^{n}\frac{a_k}{10^{k!}}=\frac{a_1 10^{n!-1!}+a_2 10^{n!-2!}+\cdots+a_n}{10^{n!}}=\frac{p_n}{q_n}\in K$$

$$\therefore\quad 0<\xi-\frac{p_n}{q_n}=\frac{a_{n+1}}{q_n^{n+1}}+\frac{a_{n+2}}{q_n^{(n+1)(n+2)}}+\frac{a_{n+3}}{q_n^{(n+1)(n+2)(n+3)}}$$

$$+\cdots\leqslant\frac{1}{q_n^n}\left(\frac{9}{10^{n!}}+\frac{9}{10^{2\cdot n!}}+\frac{9}{10^{3\cdot n!}}+\cdots\right)$$

$$<\frac{1}{q_n^n}\left(\frac{9}{10}+\frac{9}{10^2}+\frac{9}{10^3}+\cdots\right)$$

$$=\frac{1}{q_n^n}\leqslant\frac{1}{q_n^{N+1}}\ (n>N)$$

与前面的证明一样，ξ是一个超越数．这样的超越数有无穷多个．历史上有人把这种超越数叫做柳维尔（Liouville）超越数．

我们知道有理数集K是一个可数集合，[0,1]中一切实数的集合是一个不可数集合。可数集合的含有无限多个元素的子集亦可数集合；不可数集合的任一扩集亦不可数．在集合论中还有下列常用的定理：每一个无穷集都包含可数的真子集；可数个两两无交的有穷集的并集是一个可数集，有限个可数集的并集或可数个可数集的并集是可数集等等．

定理7·7 一切代数数所构成的集合A是一个可数集．

证明 首先证明全体整系数（有理整数为系数）本原不可约多项式

$$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n,\quad a_i\in R(i=0,\ 1,\ \cdots,n)$$

的根的集合是一个可数集．令

$$h_f=n+|a_0|+|a_1|+\cdots+|a_n|$$

为f(x)的高（high）．显然给定高h的整系数不可约的本原多项式的个数是有限的，其根的总数也是有限的，用M_h表示全体这些根的集合，则M_h是一个有限集．全体整系数本原不可约多项式的根的集合，是可数个两两无交的有限集$M_0=\{0\}$，$M_1=\{1,\ -1\}$，M_2，…，M_h，…的并集，它仍然是一个可数集．即

$$M=\bigcup_{h=0}^{\infty}M_h$$

是一个可数集。实际上，

$$f(x)=a_0\left(x^n+\frac{a_1}{a_0}x^{n-1}+\cdots+\frac{a_n}{a_0}\right)$$
$$=a_0(x^n+b_1x^{n-1}+\cdots+b_n)$$
$$=a_0g(x)\quad(b_i\in K)$$

$g(x)$是有理数域上的首项系数为1的不可约多项式。它的根与$f(x)$的根完全一致。由定义7·1知道，M就是一切代数数的集合。即$A=M$是可数集。

系1 全体超越数的集合是不可数集。

证明 在集合论中已知，全体实数的集合是不可数集合，复数集是实数集的扩集，故复数集C亦不可数集。一切超越数集合T和一切代数数集合A，是C的两个不相交的子集，且

$$C=A\cup T$$

若T是可数集，则$A\cup T=C$也是可数集。这是不可能的。所以T是不可数集。

系2 一个不可数集与可数集的并集是不可数集。

系3 一切非超越数的实无理数的集合是可数集。

证明 一切实代数数的集合S是代数数集A的无限真子集，故S是一个可数集。S中包括一切非超越数的实无理数的集合F，和有理数集K。即F和K是S的两个无限真子集，且

$$S=F\cup K$$

所以F是可数集。否则，若F是不可数集，则S是不可数集，就得出矛盾。

第二节　二次整数的因数分解

与有理整数类似，本节将探讨二次代数整数（简称二次整数，本节所指的代数数或代数整数，都是二次的）的整除性，素代数整数（简称素数）的概念，及$R[\sqrt{m}]$中唯一分解的存在性定理等。

定义7·5　设$\overline{R}$是一个代数整数环，$\alpha\in\overline{R}$，$\beta\in\overline{R}$，若存在$\gamma\in\overline{R}$使得$\alpha=\beta\cdot\gamma$成立，则称β整除α，记作$\beta|\alpha$；或称α被β整除，记作$\alpha\vdots\beta$。β叫做α的因数，α叫做β的倍数。

若$\varepsilon\in\overline{R}$，且$\varepsilon|1$，则$\varepsilon$叫做$\overline{R}$的一个单位（unity）。

若$\alpha\in\overline{R}$，$\beta\in\overline{R}$且$\alpha=\varepsilon\beta$，ε是$\overline{R}$的单位，则称α和β是相伴的（associated）或称β是α的相伴数（β are the associate of α）。

例7·2　在$R[\sqrt{-5}]$中，$6=(1+\sqrt{-5})(1-\sqrt{-5})=2\times3$，故$1\pm\sqrt{5}|6$，$2|6$，$3|6$，$\pm1$是它的单位。

在$R[\sqrt{-3}]$中，$2\pm\sqrt{-3}|7$。±1，$\pm\frac{1}{2}(\sqrt{-3}\pm1)$是$R[\sqrt{-3}]$的六个单位。而和$2+\sqrt{-3}$相伴的数有$-2-\sqrt{-3}$，$\pm\frac{1}{2}(\sqrt{-3}+1)(2+\sqrt{-3})=\pm\frac{1}{2}(3\sqrt{3}-1)$，$\pm(\sqrt{-3}-1)(2+\sqrt{-3})=\pm\frac{1}{2}(\sqrt{-3}-5)$。

在$R[\sqrt{-1}]=R[i]$中，$1\pm i|2$；±1，$\pm i$是$R[i]$的四个单位，和$a+bi$相伴的数有$-(a+bi)$，$\pm(b-ai)$。

为了以下的应用，我们在二次数域内引进范数的概念。

定义7·6　若$\xi=a+b\sqrt{m}$，$\xi\in K(\sqrt{m})$，则称$|a^2-b^2m|$为ξ的范数（norm）。记作

$$N(\xi)=|a^2-b^2m|$$

范数有下列诸性质：

1° 若 ξ 是代数数，则 $N(\xi)$ 是非负有理数。这是显然的。

2° ξ 是代数整数时，$N(\xi)$是非负有理整数。

证明 若 $m\equiv 2$，$3\ (\mathrm{mod}\ 4)$ 时，则 $\xi=a+b\sqrt{m}\in R[\sqrt{m}]$，$a$，$b\in R$，从而 $N(\xi)=|a^2-b^2m|\geqslant 0$，$N(\xi)\in R$；若$m\equiv 1\ (\mathrm{mod}4)$ 时，则$\xi=\left(a-\frac{b}{2}\right)+\frac{b}{2}\sqrt{m}$，从而 $N(\xi)=\left|a^2-ab-b^2\left(\frac{m-1}{4}\right)\right|$是非负有理整数。

3° 当且仅当 $\xi=0$时，$N(\xi)=0$

直接计算容易得到

4° $N(\xi\eta)=N(\xi)N(\eta)$

我们称 $\overline{\xi}=r-s\sqrt{m}$ 为 $\xi=r+s\sqrt{m}$ 的共轭数（conjugate number）。若 $\xi=a+b\omega(a, b\in R)$是代数整数，其中：当$m\equiv 2$，$3(\mathrm{mod}4)$时，$r=a$，$s=b$；当$m\equiv 1\ (\mathrm{mod}\ 4)$时，$r=a-\frac{b}{2}$，$s=\frac{1}{2}b$。于是我们得到与定义 7·6 等价的范数公式。

5° $N(\xi)=N(\overline{\xi})=|\xi\overline{\xi}|$

因此，我们可以把定义7·6中范数的概念推广到n次代数数情形：若 ξ 是 n 次代数数，$\xi=\xi_1$，ξ_2，…，ξ_n 是 ξ 的共轭数。则称

$$N(\xi)=|\xi_1\xi_2\cdots\xi_n|$$

为 ξ 的范数。显然上面性质1°—4°仍然成立。

定理7·8 ε 是$R[\sqrt{m}]$的单位的充要条件是 $N(\varepsilon)=1$。

证明 若ε是$R[\sqrt{m}]$的单位，则有ε'使$\varepsilon\varepsilon'=1$，由性质4°及2°得到

$N(\varepsilon\varepsilon')=N(\varepsilon)N(\varepsilon')=N(1)=1$ 从而，有$N(\varepsilon)=1$。

反之，若$N(\varepsilon)=1$，设$\varepsilon=r+s\sqrt{m}$，则

$$N(\varepsilon)=|r^2-s^2m|=1$$

令$\varepsilon'=\pm(r-s\sqrt{m})$，可取"$\pm$"中之一，使得

$$\varepsilon\varepsilon'=\pm(r^2-s^2m)=|r^2-s^2m|=1$$

这样的ε'也是代数整数。事实上，ε'是多项式

$$x^2-2(\pm r)x+(r^2-s^2m)\quad (r,\ m\in R)$$

的根。所以ε是$K[\sqrt{m}]$的单位。

系 1 若α，β是$R[\sqrt{m}]$中一对相伴的数，则

$$N(\alpha)=N(\beta)$$

证明 设ε是$R[\sqrt{m}]$的一个单位，若$\alpha=\varepsilon\beta$，则$N(\alpha)=N(\varepsilon)N(\beta)=N(\beta)$。

系 2 若ε_1和ε_2是两个单位，则$\varepsilon_1\varepsilon_2$与$\frac{\varepsilon_1}{\varepsilon_2}$也是单位。

证明 因为ε_1，ε_2是两个单位，所以分别存在ε_1'，ε_2'使$\varepsilon_1\varepsilon_1'=1$，$\varepsilon_2\varepsilon_2'=1$，则$\varepsilon_1\varepsilon_2\varepsilon_1'\varepsilon_2'=1$，从而$\varepsilon_1\varepsilon_2|1$。所以$\varepsilon_1\varepsilon_2$是一个单位。

由于$\varepsilon_2'=\frac{1}{\varepsilon_2}$也是一单位，故$\varepsilon_1\cdot\frac{1}{\varepsilon_2}=\frac{\varepsilon_1}{\varepsilon_2}$是一个单位。

系 3 若ε是单位，则ε^n，$n\in R$亦是一个单位。

定理7·9 若$m<0$，则$R[\sqrt{m}]$中只有有限个单位，在$R[i]$中有四个，$R[\sqrt{-3}]$中有六个，其他情况有二个。

证明 令$m=-\mu(\mu>0)$。当$\varepsilon=a+b\sqrt{m}$是$R[\sqrt{m}]$

的单位时，由定理7·8知，其充要条件是 a，b 满足下面不定方程：

$$a^2+\mu b^2=1, \text{当} m\equiv 2,\ 3(\mathrm{mod}\ 4)\text{即} \mu\equiv 2,\ 1(\mathrm{mod} 4)\text{时}$$

$$\left(a-\frac{1}{2}b\right)^2+\frac{1}{4}\mu b^2=1,\ \text{当} m\equiv 1\ (\mathrm{mod} 4),$$

$$\text{即}\mu\equiv 3(\mathrm{mod}\ 4)$$

上面二方程都只有有限组整数解．事实上，第一个方程当 $\mu=1$ 时，有且只有 $(a,\ b)=(\pm 1,\ 0),\ (0,\ \pm 1)$ 四个解，所以 $R[i]$ 中有且只有四个单位：$\pm 1,\ \pm i$；$\mu>1$ 时，有且只有 $(a,\ b)=(\pm 1,\ 0)$ 两个解，所以当 $m\equiv 2,\ 3(\mathrm{mod} 4)$ 且 $m<0$ 时，$R[\sqrt{m}]$ 中有且只有 ± 1 两个单位．

第二个方程，当 $\mu=3$ 时，是 $a^2-ab+b^2=1$，

则 $$a=\frac{1}{2}(b\pm\sqrt{4-3b^2})$$

有且只有 $(a,\ b)=(\pm 1,\ 0),\ (0,\ \pm 1),\ (1,\ 1),\ (-1,\ -1)$ 六个解．所以 $R[\sqrt{-3}]$ 中有且只有 $\pm 1,\ \pm\frac{1}{2}(\sqrt{-3}-1),\ \pm\frac{1}{2}(\sqrt{-3}+1)$ 六个单位．

当 $\mu=3+4k(k\geqslant 1)$ 时，第二个方程是 $a^2-ab+(k+1)b^2=1$，于是 $a=\frac{1}{2}(b\pm\sqrt{4-(4k+3)b^2})$，有且只有 $(a,\ b)=(\pm 1,\ 0)$ 两个解，所以 $R[\sqrt{m}]$ 中有且只有两个单位 ± 1．

当 $m>0$ 时，由于 $a^2-mb^2=1$ 或 $a^2-mb^2=-1$ 往往有无限多组解，因此 $R[\sqrt{m}]$ 往往有无限多个单位．

定理7·10 在 $R[\sqrt{2}]$ 中有无限多个单位．它们的全体是：$\pm\omega^n,\ \pm\omega^{-n}(n=0,\ 1,\ 2,\ \cdots)$，其中 $\omega=1+\sqrt{2}$，$\omega^{-1}=-\overline{\omega}=-1+\sqrt{2}$．

证明 因为$N(\xi)=|a^2-2b^2|$，所以由不定方程

$$a^2-2b^2=1 \text{ 或 } a^2-2b^2=-1 \tag{9}$$

的一切整数解（a，b）所得到的$\xi=a+b\sqrt{2}$都是$R[\sqrt{2}]$的单位。

第一个方程$a=\pm\sqrt{1+2b^2}$有解：（±1，0），（±3，±2），（±17，12），…；第二个方程有解：（±1，±1），（±7，±5），（±41，±29），…。事实上，$R[\sqrt{2}]$有单位$\omega=1+\sqrt{2}$，$\omega^{-1}=-1+\sqrt{2}$，则由定理7·8的系3及系2知道。

$$\pm\omega^n,\ \pm\omega^{-n}\ (n=0,\ 1,\ 2,\ \cdots) \tag{10}$$

都是$R[\sqrt{2}]$的单位。

上面证明(10)包括$R[\sqrt{2}]$中的一切单位。

(i) 我们首先证明1与ω之间不存在其他单位ε。否则，我们将有

$$1<x+y\sqrt{2}=\varepsilon<1+\sqrt{2} \tag{a}$$

并且满足

$$x^2-2y^2=\pm1$$

$$\Longrightarrow(x-y\sqrt{2})(x+y\sqrt{2})=\pm1$$

由(a)及上式，得

$$|x-y\sqrt{2}|<1$$

$$\Longrightarrow -1<x-y\sqrt{2}<1 \tag{b}$$

(a)+(b)得

$$0<2x<2+\sqrt{2} \tag{c}$$

因而$x=1$，代入(a)得，$1<1+y\sqrt{2}<1+\sqrt{2}$即$0<y\sqrt{2}<\sqrt{2}$亦即$0<y<1$。这样的有理整数y是不存在的，也就是不存在有理整数x，y使得不等式(a)成立。

(ii) 若单位 $\varepsilon>0$，则或者 $\varepsilon=\omega^n$，或者对于某一整数n

$$\omega^n<\varepsilon<\omega^{n+1} \qquad (\mathrm{d})$$

之一必然发生．若(d)成立，把(d)的各边同乘以 $\omega^{-n}(>0)$，得

$$1<\omega^{-n}\varepsilon<\omega \qquad (\mathrm{d}')$$

由定理7·8的系2知道 $\omega^{-n}\varepsilon$ 也是 $R[\sqrt{2}]$ 的单位，故由(i)知道(d′)不成立，即(d)不成立，所以 $\varepsilon=\omega^n$．因此每一个正单位都是 $\omega^n(n=0,\ \pm1,\ \pm2,\ \cdots)$．

若 ε 是单位则 $-\varepsilon$ 亦是单位．若 $\varepsilon>0$，则 $\varepsilon=\omega^n$，可得 $-\varepsilon=-\omega^n$；若 $\varepsilon<0$，则 $-\varepsilon>0$ 从而 $-\varepsilon=\omega^n$，即 $\varepsilon=-\omega^n$．故定理得证．

令 $N'(\omega)=\omega\overline{\omega}=1^2-\sqrt{2}^2=-1$，故 $(a,\ b)=(1,\ 1)$ 是(9)的第二个方程的解；$N'(\omega^2)=(\omega\overline{\omega})^2=1$，$\omega^2=3+2\sqrt{2}$，故 $(a,\ b)=(3,\ 2)$ 是(9)的第一个方程的解．一般地，$N'(\omega^{2n+1})=-1$，$N'(\omega^{2n})=1$，这就证明了

系 (9)的第一个方程的一切整数解，可由

$$x+y\sqrt{2}=\pm(1+\sqrt{2})^{2n}$$

给出，其中 x 等于右边的整数部分 a，y 等于右边 $\sqrt{2}$ 的系数 b，并且(9)的第二个方程的一切整数解可由

$$x+y\sqrt{2}=\pm(1+\sqrt{2})^{2n+1}$$

给出．这里的 n 是任意有理整数．

当 m 是没有平方因子的正有理整数时，不定方程

$$x^2-my^2=1 \qquad (11)$$

都有无限多组解，这些解可以由 $\sqrt{m}$ 的连分数求出．例如，特别简单的

$$\sqrt{2}=[1, 2, 2, 2, \cdots]=[1, \dot{2}],$$

它的渐近分数 P_n/Q_n 是（参考第一章第三节）

a_n		1	2	2	2	2	2	2	…
P_n	1	1	3	7	17	41	99	239	…
Q_n	0	1	2	5	12	29	70	169	…

其中 $P_n=2P_{n-1}+P_{n-2}$，$Q_n=2Q_{n-1}+Q_{n-2}$（$n\geqslant 2$）。令

$$\phi_n=P_n+Q_n\sqrt{2},\quad \psi_n=P_n-Q_n\sqrt{2} \tag{e}$$

则

$$\phi_n=2\phi_{n-1}+\phi_{n-2},\quad \psi_n=2\psi_{n-1}+\psi_{n-2}\ (n\geqslant 3)$$

$$\phi_2=2\phi_1+1,\quad \psi_2=2\psi_1+1$$

由于

$$\phi_1=1+\sqrt{2}=\omega,\quad \phi_2=\omega^2;\quad \psi_1=-\omega^{-1},\quad \psi_2=\omega^{-2}$$

所以

$$\omega^2-2\omega-1=0,\quad (-\omega)^{-2}-2(-\omega)^{-1}-1=0$$

于是对于任给 $n\geqslant 2$ 都有

$$\omega^n=2\omega^{n-1}+\omega^{n-2},\quad (-\omega)^{-n}=2(-\omega)^{-n+1}+(-\omega)^{-n+2}$$

所以，用数学归纳法容易证明

$$\phi_n=\omega^n=P_n+Q_n\sqrt{2},\quad \psi_n=(-\omega)^{-n}=P_n-Q_n\sqrt{2}$$

（$n>0$）

$$\therefore\begin{cases}P_n=\dfrac{1}{2}\{\omega^n+(-\omega)^{-n}\}=\dfrac{1}{2}\{(1+\sqrt{2})^n+(1-\sqrt{2})^n\}\\[2ex] Q_n=\dfrac{\sqrt{2}}{4}\{\omega^n-(-\omega)^{-n}\}=\dfrac{\sqrt{2}}{4}\{(1+\sqrt{2})^n-(1-\sqrt{2})^n\}\end{cases} \tag{f}$$

由(e)及(f)得

$$P_n^2 - 2Q_n^2 = \phi_n\psi_n = (-1)^n \quad (g)$$

由(g)知道$\sqrt{2}$偶次的渐近分数P_{2k}/Q_{2k}给出(9)的第一个方程的解；奇次渐近分数P_{2k+1}/Q_{2k+1}给出(9)的第二个方程的解。

若$x^2-2y^2=1$，并且$\frac{x}{y}>0$，则

$$0<\frac{x}{y}-\sqrt{2}=\frac{1}{y(x+y\sqrt{2})}<\frac{1}{y\cdot 2y\sqrt{2}}<\frac{1}{2y^2}$$

于是$\frac{x}{y}$是$\sqrt{2}$的一个渐近分数，其证法这里不作介绍，必要时读者可参阅Hardy and Wright:《An Introduction to the Theory of Numbers》中定理184。

用连分数的渐近分数亦能给出方程(11)的全部解，但其证明很不容易。一般地，只能从$\sqrt{m}$的某些渐近分数给出$R[\sqrt{m}]$的单位。例如，$\sqrt{6}=[1, \dot{2}, \dot{4}]$它的渐近分数

$$\frac{P_n}{Q_n}=\frac{2}{1}, \frac{5}{2}, \frac{22}{9}, \frac{49}{20}, \frac{218}{89}, \frac{485}{198}, \frac{2158}{881}, \frac{4801}{1960}, \cdots$$

其中偶次渐近分数$\frac{x}{y}=\frac{5}{2}, \frac{49}{20}, \frac{485}{198}, \frac{4801}{1960}, \cdots$等都给出$x^2-6y^2=1$的解，但奇次渐近分数既不能给出$x^2-6y^2=1$的解，也不能给出$x^2-6y^2=-1$的解，并且此时$x^2-6y^2=-1$是无解的。否则，x，y必为一奇一偶的，若$x=2k+1$，$y=2h$，则$4k(k+1)+1=24h^2-1$而$4k(k+1)-1\equiv-1 \pmod 8$，$24h^2-1\equiv 1 \pmod 8$，故$(x, y)$不是$x^2-6y^2=-1$的解；若$x=2k$，$y=2h+1$，则$4k^2=24h(h+1)-5$，这是不可能的。

定义7·7 设$\overline{R}$是一个代数整数环，$\forall\alpha\in\overline{R}$，$\alpha$不是单位，若$\alpha$除单位及$\alpha$的相伴数之外，不被$\overline{R}$中其他数所整除，则$\alpha$叫做$\overline{R}$的素代数整数，简称素数。否则，$\alpha$叫做$\overline{R}$的合代数整数，简称合数。

例7·3 (i) 2是$R[\sqrt{-5}]$的素数。若

$$2=(a_1+b_1\sqrt{-5})(a_2+b_2\sqrt{-5}),\ a_1,\ b_1,\ a_2,\ b_2\in R$$

则
$$4=N(2)=N(a_1+b_1\sqrt{-5})N(a_2+b_2\sqrt{-5})$$
$$=\left(a_1^2+5b_1^2\right)\left(a_2^2+5b_2^2\right)$$

显然$a_1^2+5b_1^2\neq 2$，故$a_1^2+5b_1^2=4$或1。

若$a_1^2+5b_1^2=4$，则$a_1=\pm 2$，$b_1=0$，于是$a_1+b_1\sqrt{-5}$是2的相伴数；

若$a_1^2+5b_1^2=1$，则$a_1+b_1\sqrt{-5}$是$R[\sqrt{-5}]$的单位，而且$a_2^2+5b_2^2=4$，于是$a_2+b_2\sqrt{-5}$是2的相伴数。所以2是$R[\sqrt{-5}]$的素数。

但$2=(1+i)(1-i)$，而$1+i$，$1-i$都不是2的相伴数，故2是$R[i]$的合数。

(ii) $41=(6+\sqrt{-5})(6-\sqrt{5})$，而$N(6+\sqrt{-5})=N(6-\sqrt{-5})=41$，不是$R[\sqrt{-5}]$的单位，所以41是$R[\sqrt{-5}]$的合数。

(iii) 在$R[\sqrt{-5}]$中

$$6=2\times 3=(1+\sqrt{-5})(1-\sqrt{-5})$$

而2，3，$1+\sqrt{-5}$，$1-\sqrt{-5}$都是$R[\sqrt{-5}]$的素数，$N(2)=$

4，$N(3)=9$，$N(1\pm\sqrt{-5})=6$．由定理7·8的系1知道，$1\pm\sqrt{-5}$不是2或3的相伴数．故在$R[\sqrt{-5}]$中唯一分解定理不成立．

定理7·11 若$\alpha\neq 0$是$R[\sqrt{m}]$中不是单位的一个数，则α一定能分解成$R[\sqrt{m}]$的素数的乘积．

证明 若α是$R[\sqrt{m}]$的素数，则定理成立．若α是合数，则由定义7·7知，存在α_1，$\alpha_2\in R[\sqrt{m}]$，使得

$$\alpha=\alpha_1\alpha_2,\quad 1<N(\alpha_1)<N(\alpha),\quad 1<N(\alpha_2)<N(\alpha)$$

若α_1，α_2是素数，则定理已证，否则把α_1，α_2继续分解因数，其因数的范数必小于$N(\alpha_1)$或$N(\alpha_2)$．由于$N(\alpha)$是一个有限的正有理整数，所以有限次后必出现

$$\alpha=\gamma_1\gamma_2\cdots\gamma_s$$

其中$\gamma_i=(i=1,\cdots,s)$都是素数．

这个定理指出了，一个非0的二次整数，都可以分解成素数之积，但是从例7·3(iii)知道，其分解式不一定是唯一的．这样就提出了一个问题，在什么条件下，其分解式是唯一的呢？

由于在$R[\sqrt{-5}]$中唯一分解定理被破坏，并从而在$R[1]=R$中成立的某些其它定理亦被破坏．例如，α，$\beta\in R$，$(\alpha,\beta)=1$，则存在λ，$\mu\in R$，使得

$$\alpha\lambda+\beta\mu=1$$

的定理，在$R[\sqrt{-5}]$中被破坏了．譬如，3和$1+\sqrt{-5}$是$R[\sqrt{-5}]$中互不相伴的素数，则

$$3(a+b\sqrt{-5})+(1+\sqrt{-5})(c+d\sqrt{-5})=1$$

$$\Longrightarrow 3a+c-5d=1,\quad 3b+c+d=0$$

$$\Longrightarrow 3(a-b-2d)=1$$

这是不可能的。

例7·4 因为$10\equiv 2 \pmod 4$，所以$R[\sqrt{10}]$的任一数都具有形状：$a+b\sqrt{10}$，a，$b\in R$。而

$$6=2\times 3=(4+\sqrt{10})(4-\sqrt{10})$$

容易证明，2，3，$4+\sqrt{10}$，$4-\sqrt{10}$是$R[\sqrt{10}]$的四个素数。以2为例，若有

$$2=(a+b\sqrt{10})(c+d\sqrt{10})$$

则有
$$4=|a^2-10b^2||c^2-10d^2|$$

如果$a+b\sqrt{10}$和$c+d\sqrt{10}$不是单位，必有$a^2-10b^2=\pm 2$，这是不可能的。否则$a^2\equiv\pm 2 \pmod{10}$有解，但± 2是模10的平方非剩余（$\because 1^2$，2^2，3^2，4^2，5^2，6^2，7^2，8^2，9^2，$\equiv 1$，4，9，6，5，6，9，4，$1 \pmod{10}$）。

在$R[\sqrt{10}]$中算术基本定理也被破坏。2和$4-\sqrt{10}$是不相伴的素数，则

$$2(a+b\sqrt{10})+(4-\sqrt{10})(c+d\sqrt{10})=1$$

$$\Longrightarrow 2a+4c-10d=1,\quad 2b-c+4d=0$$

$$\Longrightarrow 2(a+4b+3d)=1$$

这是不可能的。

下面将讨论唯一分解定理的存在条件。

定义7·8 任给α，$\beta\in R[\sqrt{m}]$，$\beta\neq 0$，若存在$\delta\gamma\in R[\sqrt{m}]$，使得

$$\alpha=\delta\beta+\gamma,\quad N(\gamma)<N(\beta)$$

则称$R[\sqrt{m}]$为有辗转相除法的二次整数环，亦称欧几里德二次整数环（Euclidean quadratic integers ring）简称欧氏环。

若$R[\sqrt{m}]$是欧氏环，不难仿照第一章的方法推出算术

基本定理在$R[\sqrt{m}]$中成立，亦即在$R[\sqrt{m}]$中每一个非零非单位的数，都可以唯一地（相伴数看作相同，不计因子顺序）表示为素数的乘积。

定理7·12 在任一欧氏环中，算术基本定理成立。（证明略）

对于$m<0$情况的复欧氏环的证明比较简单，而$m>0$情况的实欧氏环的证明就十分困难了。但当$m\equiv 2, 3 \pmod{10}$，还比较容易证明，只有有限个欧氏环。而$m\equiv 1 \pmod 4$的二次整数环是否欧氏环是一个核心问题，这个问题1938年由我国数学家柯召与外国数学家爱多士（Erolös），海尔伯朗（Heilbron）予以肯定的回答，我国数学家华罗庚和闵嗣鹤先后定出m的上限。到1948年这个问题被卡特兰（Chatl-and）与德汶普特（Davenport）所完全解决了，其结论是：$R[\sqrt{m}]$，当$m>0$时为欧氏环者，有且只有16个，即

$m=2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$

今初步探讨如下：

在定义7·8中知道，任一欧氏环$R[\sqrt{m}]$，任给$\xi\in K(\sqrt{m})$，则$\xi=\alpha/\beta\,(\beta\neq 0)$，$\alpha,\beta\in R[\sqrt{m}]$，存在$\delta,\gamma\in R[\sqrt{m}]$，使得$N(\xi-\delta)<1$。因为$\alpha=\beta\delta+\gamma$，$N(\gamma)<N(\beta)$ $\Longrightarrow \xi-\delta=\frac{\gamma}{\beta}$，$N\left(\frac{\gamma}{\beta}\right)<1\Longrightarrow N(\xi-\delta)<1$。因而定义7·8等价于

引理 设$R[\sqrt{m}]$是一个欧氏环，对于任意$\xi\in K(\sqrt{m})$则存在$\delta\in R[\sqrt{m}]$，使得

$$N(\xi-\delta)<1 \tag{12}$$

设$\xi=r+s\sqrt{m}$，$r,s\in K$。若$m\equiv 2,3 \pmod 4$，则在欧

氏环R$[\sqrt{m}]$中存在$\delta=x+y\sqrt{m}$，$x,y\in R$，使得

$$|(r-x)^2-m(s-y)^2|<1 \qquad (12)'$$

若$m\equiv 1\ (\mathrm{mod}\,4)$，则

$$\delta=x+y+\frac{1}{2}y(\sqrt{m}-1)$$

$$=(x+\frac{1}{2}y)+\frac{1}{2}y\sqrt{m}$$

于是当x，$y\in R$时，(12)变为

$$\left|\left(r-x-\frac{1}{2}y\right)^2-m\left(s-\frac{1}{2}y\right)^2\right|<1^{*} \qquad (12'')$$

当$m=-\mu<0$，容易得到

定理7·13 在复二次整数环中，刚好有五个欧氏环。即

$$m=-1,\ -2,\ -3,\ -7,\ -11.$$

证明 由于ξ的任意性，要求对于任一$\xi=r+s\sqrt{m}$，都存在$\delta\in R[\sqrt{m}]$，使得等式(12成立。有两种情况：

(i)当$m\not\equiv 1\ (\mathrm{mod}\,4)$时，取$\{r\}=\frac{1}{2}$，$\{s\}=\frac{1}{2}$，$x=[r]$，$y=[s]^{**}$，由(12′)知，要求u是满足

$$\frac{1}{4}+\frac{1}{4}u<1$$

的自然数。所以有且只有$u=1,2$，即$m=-1,-2$两个解。

(ii) 当$m\equiv 1\ (\mathrm{mod}\,4)$时，给定$\xi=r+s\sqrt{m}$，找一个y使得

---

* 这里是对(4)式中取$a=x+y$，$b=y$，而得到如上的形式。

** 对任给的$\xi\in K(\sqrt{m})$，选取$x+y\sqrt{m}\in R[\sqrt{m}]$使它满足(12′)。为了使$|r-x|$，$|s-y|$达到最大值$\xi$要选取$\{r\}=\frac{1}{2}\{s\}=\frac{1}{2}$，为了使$|r-x|$ $|s-y|$达到最小值，$x+y\sqrt{m}$要选取$x=[r]$，$y=[s]$。

$$|2s-y|\leqslant\frac{1}{2}$$

并且有一个x，使得

$$|r-x-\frac{1}{2}y|\leqslant\frac{1}{2}$$

此时可取$\{s\}=\frac{1}{4}$，$y=[2s]=2[s]$，$\{r\}=\frac{1}{2}$，$x=[r]-[s]$使上二不等式的左边取最大值。于是由(12)″得

$$\frac{1}{4}+\frac{1}{16}u\leqslant 1\text{，}u\equiv 3\pmod 4$$

当且仅当$u=3$，7，11时，满足上不等式。即$m=-3$，-7，-11。

综合上述，当且仅当$m=-1$，-2，-3，-7，-11时，$R[\sqrt{m}]$是复欧氏环。

但是，有些二次整数环中的算术基本定理成立〔这样环$R[\sqrt{m}]$的扩域$K(\sqrt{m})$叫做单域（Simple field）〕，而辗转相除法却不能进行。例如，$R[\sqrt{-19}]$和$R[\sqrt{-43}]$都不能进行辗转相除法。故此算法仅是唯一分解的充分条件而不是必要条件。可唯一分解的二次整数环有：

$m=-1$，-2，-3，-7，-11，-19，-43，-67，-163。

海尔伯朗和林佛（Lin foot）证明了最多还有一个；李莫尔（Lehmer）证明了，若还有的话，一定

$$m<-5\cdot 10^{9}$$

但是其存在的可能性是极小的。1967年巴喀尔（Baker）证明了唯一分解定理成立的虚二次整数环有且只有九个。

有更多的实欧氏环存在，已证明

定理7·14 当

$m=2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$时，$R[\sqrt{m}]$都是欧氏环，而且再也没有其他正有理整数m会使$R[\sqrt{m}]$为欧氏环。

这个定理在这里是无法证明的。

当$m=2$，或$m=3$时，由(12)′我们可以选择x和y，使得$|r-x|\leqslant\frac{1}{2}$和$|s-y|\leqslant\frac{1}{2}$，所以$R[\sqrt{2}]$是欧氏环。下面仅证明定理7·14的一部分。

定理7·15 当

$$m=2, 3, 5, 6, 7, 13, 17, 21, 29$$

时，$R[\sqrt{m}]$是欧氏环。

证明 若取

$$\lambda=0,\ n=m\ (m\not\equiv 1(\bmod 4))$$

$$\lambda=\frac{1}{2},\ n=\frac{1}{4}m\ (m\equiv 1(\bmod 4))$$

并且当$m\equiv 1(\bmod 4)$时，用2s代替s，则我们可合并(12)′和(12)″为

$$|(r-x-\lambda y)^2-n(s-y)^2|<1 \tag{13}$$

若辗转相除法在$R[\sqrt{m}]$中不成立，则不等式(13)并不经常成立，即有某些有理数r，s，使一切有理整数x，y都不满足(13)。并且我们可设*

$$0<r\leqslant\frac{1}{2},\quad 0\leqslant s\leqslant\frac{1}{2} \tag{14}$$

存在一对有理数r,s满足(14)，使得任一$x,y\in R$，都有

$$(r-x-\lambda y)^2\geqslant 1+n(s-y)^2 \qquad [P(x,y)]$$

$$n(s-y)^2 \geqslant 1+(r-x-\lambda y)^2 \qquad [N(x,y)]$$

之一成立。我们将引用下列特殊的不等式对：

$$r^2 \geqslant 1+ns^2,\ [P(0,0)],\quad ns^2 \geqslant 1+r^2,\ [N(0,0)];$$

$$(1-r)^2 \geqslant 1+ns^2,[P(1,0)],\quad ns^2 \geqslant 1+(1-r)^2,\ [N(1,0)];$$

$$(1+r)^2 \geqslant 1+ns^2,\ [P(-1,0)],\ ns^2 \geqslant 1+(1+r)^2,\ [N(-1,0)].$$

关于某些满足(14)的 r 和 s，上述每一对的不等式中至少有一个成立。若 $r=s=0$ 时，$P(0,0)$和$N(0,0)$都不成立，则应排除$(r,s)=(0,0)$的情况。

由于满足(14)且不全为 0 的 r 和 s，$P(0,0)$ 和 $P(1,0)$ 不成立，因而$N(0,0)$和$N(1,0)$成立。若$P(-1,0)$成立，则由$P(-1,0)$及$N(1,0)$给出

$$(1+r)^2 \geqslant 1+ns^2 \geqslant 2+(1-r)^2 \Longrightarrow 4r \geqslant 2 \Longrightarrow r \geqslant \frac{1}{2}$$

• 容易看出，当$m\not\equiv 1$(mbd 4)时，则(13)的左边是

$$|(r-x)^2-m(s-y)^2| \qquad (\alpha)$$

对r，x，s，y若代以

$$\varepsilon_1 r+u,\ \varepsilon_1 x+u,\ \varepsilon_2 s+v,\ \varepsilon_2 y+v,$$

其中$\varepsilon_1,\varepsilon_2$是 1 或 -1，u，υ是有理整数，(α)是不变的，因而我们可以选择适当的$\varepsilon_1,\varepsilon_2,u,\upsilon$使得$\varepsilon_1 r+n$和$\varepsilon_2 s+\upsilon$界于 0 和$\frac{1}{2}$之间。

更复杂一点的情况，当$m\equiv 1$(mod4)时，则(13)的左边是

$$\left|\left(r-x-\frac{1}{2}y\right)^2-\frac{1}{4}m(s-y)^2\right| \qquad (\beta)$$

对r，x，s，y用下列四种之一来代替，(β)是不变的。

(1)$\varepsilon_1 r+u$，$\varepsilon_1 x+u$，$\varepsilon_1 s$，$\varepsilon_1 y$；　　(2)r，$x-\upsilon$，$s+2\upsilon$，$y+2\upsilon$；

(3)r，$x+y$，$-s$，$-y$；　　(4)$\frac{1}{2}-r$，$-x$，$1-s$，$1-y$，

我们首先用(1)使$0\leqslant r\leqslant 1$。其次用(2)使$-1\leqslant s\leqslant 1$继之，若必要时用(3)使$0\leqslant s\leqslant 1$。若得到$0\leqslant s\leqslant\frac{1}{2}$，这样简化工作已完成。若$\frac{1}{2}\leqslant s\leqslant 1$，最后用(4)，因为$\frac{1}{2}-r$介于 0 和 $\frac{1}{2}$之间故对这样的 r 可以同样进行。

由上式及(14)得出 $r=\frac{1}{2}$ 且 $ns^2=\frac{5}{4}$，这是不可能的。事实上，设 $s=\frac{p}{q}$ $(p,q)=1$。若 $m\not\equiv 1\pmod 4$，则 $m=n$，并且从 m 无平方因数，$0\leqslant s\leqslant\frac{1}{2}$ 与 $ns^2=\frac{5}{4}\Longrightarrow 4mp^2=5q^2\Longrightarrow p^2|5, q^2|4m\Longrightarrow p=1$，$q=2, m=5\equiv 1\pmod 4$。这与 $m\not\equiv 1\pmod 4$ 的假设矛盾。

若 $m\equiv 1\pmod 4$，则 $m=4n\Longrightarrow mp^2=5q^2\Longrightarrow p=1$，$q=1$，$s=1$，这与条件(14)矛盾。因而 $P(-1,0)$ 不成立，所以 $N(-1,0)$ 成立。从而给出

$$ns^2\geqslant 1+(1+r)^2\geqslant 2$$

再由(14)可得 $n\geqslant 8$。

这就说明了当 $n<8$ 时，即在 $m\not\equiv 1\ (\mathrm{mod}\ 4)$ 时，$m<8$；当 $m\equiv 1\pmod 4$ 时，$m<32$ 的一切 $R[\sqrt{m}]$ 中，都可以进行辗转相除法。即当

$$m=2,\ 3,\ 5,\ 6,\ 7,\ 13,\ 17,\ 21,\ 29$$

时，$R[\sqrt{m}]$ 是欧氏环。

系　在 $R[\sqrt{23}]$ 中不能进行辗转相除法。

证明　当 $m=23$ 时，取 $r=0$，$s=\frac{7}{23}$，则(13)是

$$\left|x^2-23\left(\frac{7}{23}-y\right)^2\right|<1\Longrightarrow|23x^2-(23y-7)^2|<23$$

$\therefore$ $\xi=23x^2-(23y-7)^2\equiv -49\equiv -3\pmod{23}$，$\xi$ 必须是 -3 或20，容易看出这两个假设都是不可能的。例如，

$$\xi=23X^2-Y^2=-3 \tag{α}$$

则 $3\nmid X$ 且 $3\nmid Y$（否则 $9|(-3)$，这是不可能的），于是 $X^2\equiv 1$，$Y^2\equiv 1\pmod 3\Longrightarrow\xi\equiv 22\equiv 1\pmod 3$。对于任何有理整数对（$X,Y$），($\alpha$)均不成立。

虽然R$[\sqrt{23}]$不是欧氏环，但它的算术基本定理成立，在这里我们不能证明这个结论。

当然很难证明全体正的m，除定理7·14所列的m值之外，R$[\sqrt{m}]$都不是欧氏环。这里我们仅能证明

定理7·16 当$m\equiv 2$或$3\pmod 4$的实欧氏环R$[\sqrt{m}]$只有有限个。

证明 若$m\equiv 2$或$3\pmod 4$，R$[\sqrt{m}]$是欧氏环。在(12′)中我们取$r=0$且$s=t/m$，这里的t是由后面选取的一个有理整数，则存在有理整数x,y，使得

$$\left|x^2-m\left(y-\frac{t}{m}\right)^2\right|<1,\quad |(my-t^2)-mx^2|<m$$

因为$(my-t)^2-mx^2\equiv t^2\pmod m$,所以存在x,y，使得

$$z^2-mx^2\equiv t^2\pmod m,\quad |z^2-mx^2|<m \tag{15}$$

若$m\equiv 3\pmod 4$，我们选取t为奇数，使得

$$5m<t^2<6m$$

实际上，当m足够大时，这样的t是存在的。如，当$m=479=4\times 119+3$，取$t=49$等等。由(15)z^2-mx^2是等于t^2-5m或者t^2-6m，因此

$$t^2-z^2=m(5-x^2),\quad t^2-z^2=m(6-x^2) \tag{16}$$

之一成立，但对于模8而言，

$t^2\equiv 1$; $z^2,x^2\equiv 0$, 1或4; $m\equiv 3$或7

$\Longrightarrow t^2-z^2\equiv 0$, 1或5; $5-x^2\equiv 1$, 4或5; $6-x^2\equiv 2$, 5或6;

$m(5-x^2)\equiv 3$, 4或7; $m(6-x^2)\equiv 2$, 3, 6或7.所以无论怎样选取上述的剩余,(16)的二式都不成立。也就是说,$m=3\pmod 4$时，对充分大的m，R$[\sqrt{m}]$都不是欧氏环。

若$m\equiv2(\bmod 4)$，我们选取满足$2m<t^2<3m$的奇数t，与上面一样当m足够大时，这是可能的。如，$m=310$，取$t=25$。在这种情况下，下列二等式之一成立：

$$t^2-z^2=m(2-x^2),\ t^2-z^2=m(3-x^2) \qquad (17)$$

但是对模8而言，

$m\equiv2$或6；$2-x^2\equiv1$，2或6；$3-x^2\equiv2$，3或7

$\Longrightarrow m(2-x^2)\equiv2$，4或6；$m(3-x^2)\equiv2$，4或6此时(17)的二式都不成立。也就是说$m=2(\bmod 4)$时，充分大的m，$R[\sqrt{m}]$都不是欧氏环。

总之，若$m\equiv2$，$3(\bmod 4)$，并且m充分大时，$R[\sqrt{m}]$不是欧氏环。

与定理7·16 一样地：若$m\equiv1(\bmod 4)$，当m充分大时，$R[\sqrt{m}]$不是欧氏环，但其证明方法十分复杂，这里不再详述。

本节有关文献的介绍可参阅：Hardy and Wright：《An Introduction to The Theory of Numbers》第14章的附注。

第三节 理 想 数

从例7·3(iii)知道在$R[\sqrt{-5}]$中唯一分解定理不成立。为了解决这个问题康米尔(Kummer)于1844年引入了理想数的概念建立了理想数的理论。为了引进一般理想数的概念。先介绍

定理7·17 若ξ是一个n次代整数，则所有形如

$$a_0+a_1\xi+\cdots+a_{n-1}\xi^{n-1} \quad (a_i\in K) \qquad (18)$$

的数成一个域。且(18)的系数不同时表示不同的数(即1，ξ，…，ξ^{n-1}在K上线性无关)。

证明 若至少有一个系数$a_i \neq b_i$的等式

$$a_0 + a_1\xi + \cdots + a_n\xi^{n-1} = b_0 + b_1\xi + \cdots + b_n\xi^{n-1}$$

则ξ适合一个次数不高于n的整系数多项式，这与ξ是n次代数数的假设矛盾。故上等式不成立，即1，ξ，$\cdots\xi^{n-1}$在k上线性无关。

设$P = \{\xi = a_0 + a_1\xi + \cdots + a_{n-1}\xi^{n-1} | a_i \in K\}$，今证在P内关于复数的加、减、乘、除（0不作除数）闭合。并设ξ是有理系数不可约多项式

$$f(x) = t_0 + t_1x + \cdots + t_nx^n \ (t_i \in K, \ t_n \neq 0)$$

的根。

$$\alpha = a(\xi) = a_0 + a_1\xi + \cdots + a_{n-1}\xi^{n-1}$$

$$\beta = \xi b + b_1\xi + \cdots + b_{n-1}\xi^{n \ \ 1}$$

则

$$\alpha \pm \beta = a(\xi) \pm b(\xi) = a_0 \pm b_0 + (a_1 \pm b_1)\xi + \cdots + (a_{n-1} \pm b_{n-1})\xi^{n-1}$$

$\therefore \qquad \alpha \pm \beta \in P$

用带余除法，得

$$a(x)\cdot b(x) = f(x)g(x) + r(x) \ (\partial r < n)$$

$$\Longrightarrow \alpha\beta = r(\xi)$$

$\therefore \qquad \alpha\beta \in P$

最后，若$\beta \neq 0$，则$b(x)$与$f(x)$互素，故有有理系数多项式$g(x)$，$h(x)$，$\partial g < n$，使

$$g(x)b(x) + R(x)\ f(x) = 1$$

把$x = \xi$代入上式，得到$\frac{1}{\beta} = g(\xi) \in P$，故$\alpha \cdot \frac{1}{\beta} = \frac{\alpha}{\beta} \in P$。所以P是一个数域。

这样的P叫做n次代数数域(algebraicnumber field of

n degree）。也叫做有理数域K上添加ξ所得的单扩张（simple extension）或n次有限扩张，或代数扩张（algebraic extenion）。记作：$P=K(\xi)$。

$1, \xi, \xi^2, \cdots, \xi^{n-1}$叫做$K(\xi)$的基底（base）。

定义7·9 设$\alpha_1, \alpha_2, \cdots, \alpha_q$是$K(\xi)$中任意q个代数整数（下简称整数），则称所有形如

$\eta_1\alpha_1+\eta_2\alpha_2+\cdots+\eta_q\alpha_q$（$\eta_1, \eta_2, \cdots, \eta_q$为$K(\xi)$中的整数）的整数，所成的集合为由$\alpha_1, \alpha_2, \cdots, \alpha_q$生成的理想数（ideal）。记作：$[\alpha_1, \alpha_2, \cdots, \alpha_q]$。

由一个整数α所生成的理想数叫做主理想数（principal ideal）。记作：$[\alpha]$。

只有一个整数0所成的集合，亦成一理想数$[0]$，下面只讨论非$[0]$的理想数。

理想数$[1]$表示由$K(\xi)$中一切整数所组成的集合（这样的整数环仍用$R[\xi]$来表示）称为单位理想数。

下面我们用黑体英文字母来表示理想数。如

$\mathbf{A}=[\alpha_1, \cdots, \alpha_g]$ $\mathbf{B}=[\beta_1, \cdots, \beta_r]$，$[1]=\mathbf{D}$等等。

二理想数$\mathbf{A}=\mathbf{B}$指的是任给$\alpha\in\mathbf{A}$，都有$\alpha\in\mathbf{B}$，反之，任给$\beta\in\mathbf{B}$，都有$\beta\in\mathbf{A}$。

理想数有下列诸性质：

1° 若$\alpha, \beta\in\mathbf{A}$；$\Longrightarrow\alpha\pm\beta\in\mathbf{A}$

2° 若$\alpha\in\mathbf{A}$，$\eta\in R[\xi]\Longrightarrow\eta\alpha\in\mathbf{A}$

3° $\mathbf{A}=[\alpha_1, \cdots, \alpha_q]=\mathbf{B}=[\beta_1, \cdots, \beta_r]$

$$\Longleftrightarrow\alpha_i=\sum_{j=1}^{r}\xi_{ij}\beta_j, \beta_j=\sum_{i=1}^{q}\eta_{ji}\alpha_i \qquad (19)$$

其中$1\leqslant i\leqslant q$，$1\leqslant j\leqslant r$，$\xi_{ij}\in R[\xi]$，$\eta_{ji}\in R[\xi]$特别是：若$[\alpha]=[\beta]$，则α与β是相伴数。

上述三性质都可由定义立即得到.

设$a_1, a_2, \cdots, a_q \in R$，$d=(a_1, a_2, \cdots, a_q)$，则存在$x_1, x_2, \cdots, x_q \in R$，使得

$$d = a_1x_1 + a_2x_2 + \cdots + a_qx_q$$

所以在有理数域K中$[a_1, a_2, \cdots, a_q]=[d]$，即在K中只有主理想存在. 但在$R[\sqrt{-5}]$中$(3, 1+\sqrt{-5})=1$而不存在$\xi$，$\eta \in R[\sqrt{-5}]$，使$3\xi+(1+\sqrt{-5})\eta=1$，所以理想数$[3, 1+\sqrt{-5}]$不可能化为主理想数. 所以非主理想数的理想数是存在的。一般地

4° 在单域$K(\sqrt{m})$中的一切理想数，都是主理想数。

其证明是简单的，但必须先引入

定义7·10 理想数

$[\alpha_1\beta_1, \cdots, \alpha_1\beta_r, \alpha_2\beta_1, \cdots, \alpha_2\beta_r, \cdots; \alpha_q\beta_r]$称为理想数

$$\mathbf{A}=[\alpha_1, \cdots, \alpha_q], \mathbf{B}=[\beta_1, \cdots, \beta_r]$$

的乘积，记作：$\mathbf{A}\cdot\mathbf{B}$.

5° 定义7·10的合理性定理：**A**与**B**之积，与其生成元α_i，β_j的选择无关，即若

$$\mathbf{A}=[\alpha_1, \cdots, \alpha_q]=[\alpha'_1, \cdots, \alpha'_s]$$

$$\mathbf{B}=[\beta_1, \cdots, \beta_r]=[\beta'_1, \cdots, \beta'_t]$$

则

$$\mathbf{A}\cdot\mathbf{B}=[\alpha_1\beta_1, \cdots, \alpha_1\beta_r, \alpha_2\beta_1, \cdots, \alpha_q\beta_r]$$

$$=[\alpha'_1\beta'_1, \cdots, \alpha'_1\beta'_t, \alpha'_2\beta'_1, \cdots, \alpha'_s\beta'_t]$$

读者可应用理想数相等的定义来证明. 同样地下面有些

简单的性质，都留给读者自行证明。

6° (i) $D\cdot A=A$

(ii) 交换律：$A\cdot B=B\cdot A$

(iii) 结合律：$(A\cdot B)\cdot C=A\cdot(B\cdot C)$

用归纳法定义$A_1\cdots A_m=(A_1\cdots A_{m-1})A_m$（m是任何自然数），定义$A^0=D$。则

(iv) $A^m\cdot A^l=A^{m+l}$

$(A^m)^l=A^{ml}$

$(A\cdot B)^m=A^mB^m$

定义7·11 对二理想数A和B，若存在理想数C，使得

$$A=B\cdot C$$

则称B整除A，记作$B\mid A$。此时称B，C为A的因数。

7° (i)若$C\mid B, B\mid A\Longrightarrow C\mid A$

(ii) 若$B\mid A$，C是任何理想数，则$BC\mid AC$；

(iii) 对任何理想数A，都有

$$D\mid A, A\mid A$$

(iv) 若$B\mid A$，则$\forall\alpha\in A$，都有$\alpha\in B$。

(v) 若$A\mid D$，则$A=D$。

今只证明(iv)。令$A=B\cdot C$，而$B=[\beta_1,\cdots,\beta_r]$，$C=[\gamma_1,\cdots,\gamma_s]$，则$\forall\alpha\in A$，都有

$$\alpha=\sum_{j=1}^{r}\sum_{k=1}^{s}\eta_{jk}\beta_j\gamma_k=\sum_{j=1}^{r}\left(\sum_{k=1}^{s}\eta_{jk}\gamma_k\right)\beta_j,\ \eta_{jk}\in R[\xi]$$

于是

$$\alpha\in B$$

实际上(iv)的逆定理亦成立。若任给$\alpha\in A$，都有$\alpha\in$

B，则B|A（即下面的定理7·18系 2 ）。

由性质6° 的(iv)可得

8° 若A|D，则A＝D。

定理7·18 对于任何理想数 A，一定能找到一个理想数 B，使A·B＝〔a〕。〔a〕是由自然数 a 生成的理想数。

证明 若A 是一个主理想数，如 A＝〔α〕，则

$B = [\alpha^{(2)} \cdots \alpha^{(n)}]$，其中$\alpha^{(2)}, \cdots, \alpha^{(n)}$是α 的共轭数，于是取 $a = N(\alpha) = |\alpha\alpha^{(2)} \cdots \alpha^{(n)}|$，得

$$A \cdot B = [\alpha\alpha^{(2)} \cdots \alpha^{(n)}] = [a]$$

若$A = [\alpha_1, \cdots, \alpha_0]$不是主理想数，作多项式

$$f(x) = \alpha_1 x^1 + \cdots + \alpha_0$$

令

$$g(x) = \prod_{j=2}^{n-1} (\alpha_1^{(j)} x^1 + \cdots + \alpha_0^{(j)}) = \beta_k x^k + \cdots + \beta_0$$

其中$k = (n-1)1$，$\alpha_i^{(j)}$是 α_i 的共轭数，则取$\alpha_i^{(1)} = \alpha_i$，并由对称多项式的基本定理，得

$$f(x)g(x) = \prod_{j=1}^{n} (\alpha_1^{(j)} x^1 + \cdots + \alpha_0^{(j)})$$

$$= c_{1+k} x^{1+k} + \cdots + c_0 \ (c_i \in R)$$

令

$$a = (c_{1+m}, \cdots, c_0), B = [\beta_k, \cdots, \beta_0]$$

下面证明

$$A \cdot B = [a]$$

因对一切 $0 \leqslant h \leqslant 1 + k$，都有$a | c_h$，则$a | \alpha_\mu \beta_\nu$

$(0 \leqslant \mu \leqslant l,\ 0 \leqslant \upsilon \leqslant k)$*. 所以$\alpha_\mu \beta_\upsilon \in [a]$（性质7°(iv)）. 反之，因$a=(c_{l+k}, \cdots, c_0)$，故有有理整数$d_{l+k}, \cdots, d_0$，使

$$a = c_{l+k}d_{l+k} + \cdots + c_0 d_0$$

$$\because \quad c_h = \sum_{\substack{\mu+\upsilon=h \\ 0\leqslant\mu\leqslant l \\ 0\leqslant\upsilon\leqslant k}} \alpha_\mu \beta_\nu \ (0 \leqslant h \leqslant l+k)$$

$$\therefore \quad a = \sum_{\mu=1}^{l} \sum_{\upsilon=1}^{m} \eta_{\mu\upsilon} \alpha_\mu \beta_\upsilon \ (\eta_{\mu\upsilon} \in R[\xi])$$

所以$a \in \mathbf{A} \cdot \mathbf{B}$. 因此

$$\mathbf{A} \cdot \mathbf{B} = [a]$$

系1 若$\mathbf{A} \cdot \mathbf{C} = \mathbf{A} \cdot \mathbf{D}$，则$\mathbf{C} = \mathbf{D}$.

证明 取$\mathbf{B}$及自然数a，使

$$\mathbf{A} \cdot \mathbf{B} = [a] \Longrightarrow [a] \cdot \mathbf{C} = [a] \cdot \mathbf{D}$$

此等式的意义是$\mathbf{C}$中各数乘以a后所得的集合，与由$\mathbf{D}$中各数乘以a后所得的集合相同，所以

$$\mathbf{C} = \mathbf{D}$$

系2 若$\forall \alpha \in \mathbf{A}$，都有$\alpha \in \mathbf{B}$，则$\mathbf{B} | \mathbf{A}$.

证明 取$\mathbf{C}$及a使$\mathbf{B} \cdot \mathbf{C} = [a]$，于是$\mathbf{C} \cdot \mathbf{A}$中每一个数，都在$\mathbf{B} \cdot \mathbf{C} = [a]$中，故可令

---

* 关于代数整数的整除性，有如下的定理：令
$f(x) = \alpha_l x_e + \cdots + \alpha_0$，$\alpha_l \neq 0$；$g(x) = \beta^k x k + \cdots + \beta_0$.（$\alpha_i$，$\beta_j$是整数）又令

$$f(x)g(x) = \gamma_{l+k} x^{l+k} + \cdots + \gamma_0$$

若$\delta \in R[\xi]$，$\delta | \gamma u (0 \leqslant u \leqslant l+k)$，则

$$\delta | \alpha_v \beta_w (0 \leqslant \upsilon \leqslant l, 0 \leqslant \omega \leqslant m)$$

此定理我们用而不证，其证明可参考华罗庚著《数论导引》第十六章第五节。

$$CA=[a\gamma_1,\ \cdots,\ a\gamma_q]=[a]\cdot[\gamma_1,\ \cdots,\ \gamma_q]$$
$$=C\cdot B[\gamma_1,\cdots,\gamma_q]$$
$$\therefore\quad A=B[\gamma_1,\cdots,\gamma_q]\Longrightarrow B|A$$

定义7·12 若一理想数除D和本身外无其他因数，则称这个理想数为素理想数(prime ideal)。通常用P表示素理想数。

定理7·19 任二理想数$A=[\alpha_1,\cdots,\alpha_g]$，$B=[\beta_1,\cdots,\beta_r]$，则有唯一的理想数D，满足

（i） $D|A$，$D|B$

（ii） $D_1|A$，$D_1|B$，则$D_1|D$

换言之，D中任一数都能写成$\alpha+\beta$的形式，其中$\alpha\in A$，$\beta\in B$。

证明 取$D=[\alpha_1,\ \cdots,\ \alpha_g,\ \beta_1,\ \cdots,\ \beta_r]$则定理中的二性质被满足。事实上，此时显然有$D|A$，$D|B$。且若理想数$D_1|A$，$D_1|B$，则$D_1$含有A及B，故亦包含有D，所以$D_1|D$。

次证明，D是唯一的。若D'也具有性质（i）（ii），则

$$D'|D,\quad D|D'$$

亦即D中各数均在D'中，而且D'中各数也均在D中，所以

$$D'=D$$

又因$D=[\alpha_1,\cdots,\alpha_g,\beta_1,\cdots,\beta_r]$中任何一数，都能写成

$$\eta_1\alpha_1+\cdots+\eta_g\alpha_g+\lambda_1\beta_1+\cdots+\lambda_r\beta_r$$

的形式。令$\alpha=\eta_1\alpha_1+\cdots+\eta_g\alpha_g$，$\beta=\lambda_1\beta_1+\cdots+\lambda_r\beta_r$，则$\alpha\in A$，$\beta\in B$，因此D的任一元素都能表成$\alpha+\beta$的形

式.

定义7·13 定理7·19中的D叫做A和B的最大公因数，记作：$D=(A,B)$. 可用归纳定义的方法，定义$(A_1,\cdots,A_{m-1},A_m)=((A_1,\cdots,A_{m-1}),A_m)$，若$(A,B)=D$，则称A，B互素.

它们有如下的性质：易证

9° 若$(A,B)=D$，则对任何理想数C，都有

$$(AC,BC)=D\cdot C$$

10° 若素理想数$P|AB$，且$P\nmid A$，则$P|B$.

证明 因为$P\nmid A$，所以

$(P,A)=D\Longrightarrow(PB,AB)=B$又因$P|AB$，所以$P|B$.

11° 任何理想数都只能有有限个不同的因子.

证明 任给理想数A，存在理想数B与自然数a使得$A\cdot B=[a]$，故A中含有a，且A的任一因子亦含有a. 若能证明，含有一个固定的自然数的理想数，只可能有有限个，则性质得证.

设$M=[\alpha_1,\cdots,\alpha_m]$,为一含有a的理想，又设$\omega_1,\cdots,\omega_n$是$R[\xi]$的一组基底（亦称整基，是为了与$K(\xi)$的基底相区别），由于$\alpha_i\in R[\xi]$,

$\therefore\quad \alpha_i=g_{i1}\omega_1+\cdots+g_{in}\omega_n\ (1\leqslant i\leqslant m,\ g_{ik}\in R)$

再令 $g_{ik}=aq_{ik}+r_{ik}\ (0\leqslant r_{ik}<a)$，则由

推得$\beta_i=\sum\limits_{k=1}^{n}q_{ik}\omega_k$, $\gamma_i=\sum\limits_{k=1}^{n}r_{ik}\omega_k$

$$\alpha_i=a\beta_i+\gamma_i,$$

又因a在M中，所以

$$M=[a\beta_1+\gamma_1,\cdots,a\beta_m+\gamma_m,a]=[\gamma_1,\cdots,\gamma_m,a]$$

因为只有有限组$\gamma_1,\cdots,\gamma_m$，故含有 a 的理想数，只可能为有限个。

定理7·20 （理想数的基本定理）任一不同于D的理想数A可分解为素理想数的乘积，且若不计其排列的次序，则分解法唯一。

证明 由性质11°知道，任何理想数只可能有有限多个不同的因子，故可对A的因子个数，施行数学归纳法。

先证可以分解。若A是素理想数，则已证，否则

$$A=B\cdot C(B\neq G,C\neq D)$$

则因B，B的因子个数少于A的因子个数，故由数学归纳法，得到证明。

次证分解的唯一性。设

$$A=B_1B_2\cdots B_l=B'_1B'_2\cdots B'_m,\ m\geqslant1,\ l\geqslant1\ \text{(a)}$$

若A是素理想数，则 $l=m=1$，于是结论正确。若A非素理想数，则 $l>1$，$m>1$。因

$$B_1\mid B'_1B'_2\cdots B'_m\overset{10^\circ}{\Longrightarrow}B_1\mid B'_j\ (1\leqslant j\leqslant m)$$

故 $B_1=B'_j$，不失一般性，可设 $j=1$。由定理7·18系1，得

$$B_2\cdots B_l=B'_2\cdots B'_m$$

由归纳点假设，定理得证。

与定义3·1类似地可以定义，当$A|\alpha-\beta$时，称代数整数α,β关于模A同余。记作

$$\alpha\equiv\beta\pmod A$$

其中$A|[\alpha]$，称为A整除α，记作$A|\alpha$。易见$A|\alpha$即α

在A中的意思。

根据同余关系把$R[\xi]$的数进行分类，使得凡属于同类的整数关于模A互相同余，而属于不同类的整数，关于模A互不同余。即$\alpha-\beta\in A$时α与β关于模A属于同一类，其类数为$N(A)$，并且有如下的结论（这里不证）。

若$A=[\alpha_1,\cdots,\alpha_n]$，$\omega_1,\cdots,\omega_n$是$R[\xi]$的基底

$$\alpha_i=\sum_{j=1}^{n}a_{ij}\omega_j\quad(a_{i,j}\in R)\qquad\text{(b)}$$

则$N(A)$等于(b)系数行列式的绝对值，即

$$N(A)=\left|\,|a_{ij}|\,\right|$$

由此若对主理想$[\alpha]$的范数$N([\alpha])$，有

$$N([\alpha])=N(\alpha)$$

并且

$$N(AB)=N(A)\cdot N(B)$$

因此若将A中元素依mod AB进行分类，其类数亦等于$N(A)$，从而得到

定理7·21 若P是素理想数，$P\nmid\alpha$，则对整数α，有

$$\alpha^{N(P)-1}\equiv1\ (\mathrm{mod}\ P)$$

实际上这是费马定理在理想数中的推广。

历史上，首先由高斯把有理整数推广到高斯整数（$R[i]$中的数）及一般代数整数。在$R[i]$中唯一分解定理仍然成立，但在$R[\sqrt{-5}]$中唯一分解定理遭到破坏，为了重建唯一分解定理，引起了当时代数数论专家的兴趣。康米尔（Kammer）在1844年开始写了一系列论文创立了理想的理论。并成功地证明了费马大定理$0<p<100$除37，59，67外都成立，并研究由单位根形成的代数数。而高斯的学生狄

德金（Richard Dedekind(1831—1916)用全新的方法探讨了唯一分解定理，在他编辑的狄里克雷（Dirichlet）的《数论》（1871)的第二版的附录10中，发表了他的结果，在同书第三版、第四版的附录中，他扩展了这些结果．就是在那里他创立了现代代数数的理论（前面的方法是狄德金的思想）．

为了了解康米尔思想，我们考察$K(\sqrt{-5})$中的二次整数环$R[\sqrt{-5}]=\{a+b\sqrt{-5}\mid a,b\in R\}$．在这里我们有

$$6=2\cdot 3=(1+\sqrt{-5})(1-\sqrt{-5})$$

其中2，3，$1+\sqrt{-5}$，$1-\sqrt{-5}$都是素整数，说明这时唯一分解定理不成立．若在域$K(\sqrt{-5})$中我们引进理想数$\alpha=\sqrt{2}$，$\beta_1=(1+\sqrt{-5})/\sqrt{2}$，$\beta_2=(1-\sqrt{-5})/\sqrt{2}$则6便被唯一地分解为

$$6=\alpha^2\beta_1\beta_2$$

这时四个因子全是理想数(2，3已不是素数，$2=\alpha^2$，$3=\beta_1\beta_2$)．借助于理想数和其它素数在这个域中因子分解是唯一的（除去可逆元素的因子以后$\frac{1}{M}$是代数整数，则代数整数M就是可逆元素，如1，-1，$5-2\sqrt{6}$和$5+2\sqrt{6}$等都是可逆元…）．一般地，借助于理想数，可以证明在缺乏唯一分解定理的所有域中，普通数论的一些结果成立．

康米尔的理想数与狄德金的定义不同，它是普通的数且无一般的定义，亦与他所研究的由单位根形成的代数数不同．

狄德金采用与康米尔完全不同的方法来重建代数数域中的唯一分解定理（如本节前面所述）．他引进了代数数类去代替康米尔的理想数，为了纪念康米尔的理想数，他把它们

改称为理想。

对于代数数域它的最主要性质是理想类数，但是类数一定的代数数域，甚至虚二次数域究竟有多少，这是一个极难的问题。1967年Baker等人借助其精深的方法定出类数为1（即该整数环满足唯一分解定理）的虚二次域只有高斯所说的九个($m=-1,-2,-3,-7,-11,-19,-43,-67,-163$)，不久类数为2的虚二次域也已定出。但是类数为3，4，5，…的虚二次域还没有希望定出来。

1976年美国数学家Goldfeld发现，这个极其艰深的问题与具有复数乘法的椭圆曲线（不是椭圆！）的L函数零点性质有关。这就把类数问题化为寻找某种特殊的椭圆曲线，即其L函数有≥3阶的零点。西德年轻数学家Zagier和美国数学家B.Gross花了很大的力气来算，单求方程的计算用了100页，终于找到这种特殊的曲线，从而给每种类数h的虚二次域$K(\sqrt{-m})$的m（他们是用d代m）一个上界。这样使问题完全解决了。他们的工作还没有发表，300页的手稿很难核对，但一些大专家如，B•Mazur都肯定他们的结果，说“无疑是正确的”。

第四节　费马定理

本节将介绍某些二次整数的费马定理。

本节开始先介绍$R[i]$中的素数和几个唯一分解定理成立的二次整数环中的素数的性质。本节$R[\sqrt{m}]$都表示算术基本定理成立的二次整数环。

若π是$R[\sqrt{m}]$中的一个素数，则

$$\pi \mid N(\pi), N(\pi)=|\pi\bar{\pi}|$$

$N(\pi)$是一个被π整除的正有理整数。若z是被π整除的最小的有理整数，且$z=z_1z_2$，则

$$\pi|z_1z_2 \Longrightarrow \pi|z_1 \text{或} \pi|z_2$$

这与z的最小性矛盾，故除非z_1或z_2之一等于1这是不可能的。所以z是一个有理素数。亦即被π整除的最小的有理整数，一定是素数p。如果π整除两个有理素数p_1和p_2，则

$\pi|p_1$，$\pi|p_2 \Longrightarrow \pi|p_1x-p_2y(x, y\in R)$对适当的$x, y\in R$可使$p_1x-p_2y=1$（定理1·12），那末$\pi|1$，这与$\pi$是素数的假设矛盾。从而得到

定理7·22 $R[\sqrt{m}]$中任一素数π，都刚好是一个有理素数的因数。

由这个定理知道$R[\sqrt{m}]$中的素数，可由有理素数经过在$R[\sqrt{m}]$中的因数分解来决定。

在$R[i]$中，若$\pi=a+bi$，$\pi|p$，则$\pi\lambda=p$从而$N(\pi)N(\lambda)=p^2$，这时或者$N(\lambda)=1$，λ是单位π是p的相伴数，或者

$$N(\pi)=(a+bi)(a-bi)=a^2+b^2=p \tag{20}$$

(i) 若$p=2$，则

$$p=1^2+1^2=(1+i)(1-i)=i(1-i)^2=(-1-i)(i-1)$$

数$1+i$，$1-i$，$-1-i$，$i-1$都是$R[i]$的素数，并且后二数是前二数的相伴数。

(ii) 若$p=4m+3$，(20)不成立。因为一个有理整数的平方关于模4是同余于0或1，所以$R[i]$中具有$4n+3$形式的有理素数是一个素数。

(iii) 若$p=4m+1$，则$\left(\frac{-1}{p}\right)=1$，因而存在一个有理整数$x$，使得

$$p \mid x^2+1 \Longrightarrow p \mid (x+i)(x-i)$$

如果p是R〔i〕中的素数，那末 $p \mid x+i$ 或者 $p \mid x-i$，这是不可能的。因为$\frac{x}{p} \pm \frac{i}{p}$不是整数，所以 p 不是素数，因而 $p=\pi\lambda=(a+bi)(a-bi)=a^2+b^2$，且$N(\pi)=a^2+b^2=p$，a，$b \in R$。这就得到了定理 5·9 的一种简单的证法，但是没有给出具体求a，b的方法。

由定理5·9 给出了一种把 $p=4m+1$ 分解成两个有理整数平方和的方法，从而可求出$p=(a+bi)(a-bi)=\pi\lambda$，二因子各自的相伴数是：

$$\pi, \pi i, -\pi-\pi i; \ \lambda, \ \lambda i, -\lambda, \ -\lambda i \tag{21}$$

以(π, λ)，$(\pi i, -\lambda i)$，$(-\pi, -\lambda i)$，$(-\pi i, \lambda i)$，(λ, π)，$(\lambda i, -\pi i)$，$(-\lambda, -\pi)$，$(-\lambda i, \pi i)$等八对数之一，代替(π, λ)，这样的八次变化对应于八个方程

$$(\pm a)^2+(\pm b)^2=p, \ (\pm b)^2+(\pm a)^2=p \tag{22}$$

它们都是$a^2+b^2=p$，并且若$p=c^2+d^2=(c+di)(c-di)$，由于在R〔i〕中唯一分解定理成立，故$(c+di, c-di)$一定是上述八对数之一，这就证明了这种表示法的唯一性。从而得到比定理5·9更强的结论。

定理7·23 任一形如 $4n+1$ 的有理素数p，都可以唯一地表成两个有理整数的平方和。

从上面的讨论，又可得到

定理7·24 R〔i〕中的素数是：

(i) $1+i$ 和它的相伴数；

(ii) 形如$4m+3$的有理素数和它们的相伴数；

(iii) 形如$4m+1$的有理素数的因数$a+bi$和它们的相伴数。

首先，我们在R〔i〕中讨论费马定理，给出类似于有理整数环中定理3·7系 1 的结论，而不一般地给出定理3·7（欧拉定理）。

定义71·4 在$R[\sqrt{m}]$中，若$\gamma|\alpha-\beta$，则称α，β关于模γ同余，记作

$$\alpha\equiv\beta\ (\bmod\gamma)$$

这时，$\alpha-\beta=k\gamma$，$k\in R[\sqrt{m}]$。这个定义自然可推广到一般代数整数环$R[\xi]$中去。

下面用p和q分别代表形如$4m+1$和$4n+3$的有理素数。并且用π代表定理7·23(iii)中R〔i〕的素数。令

$$\varphi(\pi)=N(\pi)-1$$

因而$\varphi(\pi)=p-1(\pi|p)$，$\varphi(\pi)=q^2-1(\pi=q)$

定理7·25 若$(\alpha,\pi)=1$，则

$$\alpha^{\varphi(\pi)}\equiv1\ (\bmod\pi)$$

证明 设$\alpha=1+mi$，当$\pi|p$时，由$i^p=i$得

$$\alpha^p=(1+mi)^p\equiv1^p+(mi)^p=1^p+m^pi(\bmod\ p)$$

由定理3·7系 2 得

$$\alpha^p\equiv1+mi=\alpha\ (\bmod\ p)$$

因为$\pi|p$，这个同余式同样地对模π成立。消去α得

$$\alpha^{p-1}\equiv1(\bmod\pi)\Longrightarrow\alpha^{\varphi(\pi)}\equiv1(\bmod\ \pi)$$

当$\pi=q$，$i^p=-i$，且

$\alpha^p=(1+mi)^q\equiv1^q-m^qi\equiv1-mi=\overline{\alpha}(\bmod q)$类似地，$\overline{\alpha^q}\equiv\alpha(\bmod g)$，因而

$$\alpha^{p^2}\equiv\overline{\alpha}^p\equiv\alpha(\bmod q)\Longrightarrow\alpha^{q^2-1}\equiv1\ (\bmod q)$$

这个定理的证明，亦可类似于第三章第三节证明欧拉定

理一样，由于

$$1\cdot\alpha,\ 2\cdot\alpha,\cdots,(p-1)\alpha$$

是过模 p 的一个互素剩余系，因此

$$1\cdot 2\cdots(p-1)\alpha^{p-1}\equiv 1\cdot 2\cdots(p-1)\ (\mathrm{mod}\ p)$$

$$\Longrightarrow \alpha^{p-1}\equiv 1(\mathrm{mod}\ p)$$

$$\Longrightarrow \alpha^{p-1}\equiv 1(\mathrm{mod}\ \pi)$$

这里自然要与有理整数一样地，先引进模 p 的“互素剩余系”和“完全剩余系”的概念。例如，若 $\pi|p$，$\pi=a+bi$，$(a,b)=1$，a，$b\in R$，则存在 $c,d\in R$ 使得 $ad+bc=1$，而 π 的倍数

$$(a+bi)(c+di)=ac-bd+(ad+bc)i=s+i \qquad (23)$$

其中 $s=ad-bc$，于是存在 $s\in R$ 使得 $\pi|s+i$。

今考虑如下的关于模 π 互不同余的数列

$$r=0,\ 1,\ 2,\ \cdots,\ N(\pi)-1=a^2+b^2-1 \qquad (24)$$

若 $x+yi$ 是 $R[i]$ 的任一整数，有一个(24)中的 r，使得对(23)中的 s 有

$$x-sy\equiv r(\mathrm{mod}\ N(\pi))$$

则

$$x+yi\equiv y(s+i)+r\equiv r(\mathrm{mod}\ \pi)$$

(24)中的 r 过模 $N(\pi)$ 的完全剩余系，亦即它过模 π 的完全剩余系

若 α 与 π 互素，与定理3·5的证法一样 $\alpha r(r=0,\ 1,\cdots,\ a^2+b^2-1)$ 亦是过模 π 的完全剩余系。

$$\prod_{r=0}^{a^2+b^2-1}(\alpha r)\equiv\prod_{r=0}^{a^2+b^2-1}r(\mathrm{mod}\ \pi)$$

用类似的方法可证明其他情况的 $R[\sqrt{m}]$ 中相应的定理，

但是完全剩余的建立比较困难。

其次，讨论$R[\sqrt{2}]$和$R[\sqrt{5}]$中的素数，其讨论的方法和其他算术基本定理成立的环很近似。

例如，在$R[\sqrt{2}]$中，或者有理素数p是素数或者

$$N(\pi)=|a^2-2b^2|=p \tag{25}$$

的π是素数。每一个有理整数的平方都同余于0，1或4(mod8)。故当$p=8m\pm3$时，不存在满足(25)的π；当$p=8m\pm1$时，2是模p的平方剩余，即$x^2\equiv2(\mathrm{mod}\ p)$有解$x\equiv x_0(\mathrm{mod}\ p)$。取$a=x_0$，$b=1$，则$a^2-2\equiv0(\mathrm{mod}\ p)$，从而$(a-\sqrt{2})(a+\sqrt{2})\equiv0(\mathrm{mod}p)$，与定理7·24(iii)的证法一样，可知p不是$R[\sqrt{2}]$的素数，$p=\pi\lambda$，$\pi=a+b\sqrt{2}$，$\lambda=\pm(a-b\sqrt{2})$从而$N(\pi)=|a^2-2b^2|=p$。如，
$7=(3+\sqrt{2})(3-\sqrt{2})$；$17=(5+2\sqrt{2})(5-2\sqrt{2})$等等。最后，$2=\sqrt{2}^2$，$\sqrt{2}$是素数。从而得到

定理7·26 $R[\sqrt{2}]$的素数是：(i)$\sqrt{2}$；(ii)形如$8m\pm3$的有理素数；(iii)形如$8m\pm1$的有理素数的因数$a+b\sqrt{2}$。以及它们的相伴数。

$R[\sqrt{-5}]$的整数是形如$a+b\omega$，其中$a,b\in R$，而且

$$\omega=\frac{1}{2}(1+\sqrt{5})^{*},\quad N(a+b\omega)=|a^2+ab-b^2| \tag{26}$$

---

* 注意这里的ω虽与(4)式中$\omega=\frac{1}{2}(-1+\sqrt{5})$的表示法不同，但无本质上的差别，不过把ξ和N(ξ)改作$\xi=\frac{1}{2}(A+B\sqrt{m})=\frac{A-B}{2}+\frac{B}{2}(1+\sqrt{m})=a+b\omega$，其中$a=\frac{A-B}{2}$，$b=B$。$N(\xi)=$
$=|a^2+ab-b^2\frac{m-1}{4}|$。

容易证明$R[\sqrt{5}]$的一切单位是

$$\pm\omega^{\pm n}(n=0, 1, 2, \cdots) \tag{27}$$

求$R[\sqrt{5}]$的素数，依赖于方程

$N(\pi)=|a^2+ab-b^2|=p$，或$|(2a+b)^2-5b^2|=4p$

若$p=5n\pm 2$，则$(2a+b)^2\equiv\pm 3\pmod 5$，这是不可能的（$\because\left(\frac{\pm 3}{5}\right)=-1$），所以$p$是$R[\sqrt{5}]$的素数。若

$p=5n\pm 1$，则$\left(\frac{5}{p}\right)=1$，故对某些$x$,$p|x^2-5$，前面已知道，这样的$p$是可以分解因数的，最后，$5=\sqrt{5}^2=(2\omega-1)^2$。从而得到

定理7·27 $R[\sqrt{5}]$的单位是形如(27)的数，其素数是：(i)$\sqrt{5}$；(ii)形如$5n\pm 2$的有理素数；(iii)形如$5n\pm 1$的有理素数的因数$a+b\omega$。以及它们的相伴数。

同样地，可以证明费马定理：

定理7·28 若p和q分别是形如$5n\pm 1$和$5n\pm 2$的有理素数，$\varphi(\pi)=N(\pi)-1$，于是

$\varphi(\pi)=p-1(\pi|p)$；$\varphi(\pi)=q^2-1(\pi=q)$

并且$(\alpha, \pi)=1$时，则

$$\alpha^{\varphi(\pi)}\equiv 1\pmod{\pi} \tag{28}$$

$$\alpha^{p-1}\equiv 1\pmod{\pi} \tag{29}$$

$$\alpha^{p+1}\equiv\alpha\bar{\alpha}\pmod{q}，（\bar{\alpha}\text{是}\alpha\text{的共轭数}） \tag{30}$$

此外，若$\pi|p$，$\bar{\pi}$是π的共轭数，$(\alpha, \pi)=1$，则

$$\alpha^{p-1}\equiv 1\pmod{p} \tag{31}$$

证明 首先，若$2\alpha=c+d\sqrt{5}$，则

$$2\alpha^p \equiv (2\alpha)^p = (c+d\sqrt{5})^p \equiv c^p + d^p 5^{\frac{1}{2}(p-1)}\sqrt{5} \pmod p$$

但由欧拉判别条件得

$$5^{\frac{p-1}{2}} \equiv \left(\frac{5}{p}\right) = 1 \pmod p$$

且$c^p \equiv c$，$d^p \equiv d \pmod p$，因而

$$2\alpha^p \equiv (2\alpha)^p \equiv c + d\sqrt{5} = 2\alpha d(\text{mo } p) \tag{32}$$

由于 π p，故得

$$2\alpha^p \equiv 2\alpha (\bmod \pi) \tag{33}$$

因为$(2, \pi) = 1$，$(\alpha, \pi) = 1$，所以在(33)中约去2α得(29)，(32)约去2α得(31)。

类似地，若$q>2$，则

$$2\alpha^q \equiv c - d\sqrt{5} = 2\bar{\alpha} \Longrightarrow \alpha^q \equiv \bar{\alpha} (\bmod q) \tag{34}$$

$$\therefore \quad \alpha^{q+1} \equiv \alpha\bar{\alpha} = \frac{1}{4}(c^2 - 5d^2) (\bmod q) \tag{35}$$

这就证明了(30)。把(34)的右式两边q乘方得

$$\alpha^{q^2} \equiv \bar{\alpha}^q \equiv \alpha (\bmod q) \Longrightarrow \alpha^{q^2-1} \equiv 1 (\bmod q) \tag{36}$$

最后，(36)与(29)结合，且$\varphi(q) = q^2 - 1$，得(28)。

若$q = 2$时，上面证明是失败的，但是(28)和(30)仍然是成立的。若$\alpha = e + f\omega$ 而且e，f 之一是奇数，则 $N(\alpha) = |e^2 + ef - f^2|$是奇数。亦即对模2

$$\alpha^2 \equiv e^2 + f^2\omega^2 \equiv e + f\omega^2 = e + f(1+\omega) \equiv e + f(1-\omega)$$

$$= e + f\bar{\omega} = \bar{\alpha} \Longrightarrow \alpha^3 \equiv \alpha\bar{\alpha} = e^2 + ef - f^2 \equiv 1.$$

顺便地，在这里用其他方法证明斐波那契(Fibonacci)数的一个有趣性质。

我们知道，历史上斐波那契数列

$$1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ \cdots \tag{α}$$

是以无病兔子繁殖规律为例总结出来的。令

$$x=\omega=\frac{1}{2}(1+\sqrt{5}),\ y=-\frac{1}{x}=\frac{1}{2}(1-\sqrt{5}) \tag{β}$$

$$P_n=u_{n+2}=\frac{x^{n+2}-y^{n+2}}{\sqrt{5}}{}^{*},\quad Q_n=u_{n+1}=\frac{x^{n+1}-y^{n+1}}{\sqrt{5}} \tag{γ}$$

(α)的前两项 $u_1=u_2=1$，后面的任一项都是其前面两项之和，即

$$u_{n+2}=u_{n+1}+u_n(n=1,\ 2,\ \cdots) \tag{δ}$$

事实上，因为 $x+1=x^2$，$y+1=y^2$，用(γ)代入(δ)的右边经计算即得左边。

类似地，定义

$$v_n=x^n+y^n \tag{ε}$$

易得

$$v_{n+2}=v_{n+1}+v_n(n=1,\ 2,\ \cdots) \tag{ζ}$$

从而得到数列

$$1,\ 3,\ 4,\ 7,\ 11,\ 18,\ 29,\ 47,\ \cdots \tag{η}$$

通常称(η)为纳肯斯（Lucas）数列。

u_n，v_n 有如下的简单性质

1° $(u_n,\ u_{n+1})=1$，$(v_n,\ v_{n+1})=1$

2° u_n 和 v_n 或者同为奇数，或者同为偶数，并且 $(u_n,\ v_n)=1$ 或者 $(u_n,\ v_n)=2$。

---

* 因为 $\omega=\frac{1}{2}(1+\sqrt{5})=1+\frac{1}{1+}\frac{1}{1+}\cdots=[\dot{1}]$，所以 P_n/Q_n 即连分数 ω 的第 n 个渐近分数，数列(α)的各项，就是由(γ)表示的 ω 渐近分数的各分子和分母。

3° 对于任意r，都有$u_n|u_{rn}$。

4° 若$(m, n)=d$,则$(u_m, u_n)=u_d$。特别，若$(m, n)=1$，则$(u_m, u_n)=1$。

5° 若$(m, n)=1$，则$u_mu_n|u_{mn}$。

把u_n看作：

$$u_n=\frac{x^n-y^n}{x-y}$$

把 u_n，v_n 推广到n为一切整数时，则

$$u_0=0,\ v_0=0,\ u_{-n}=-(xy)^{-n}=(-1)^{n-1}u_n,\ v_{-n}=(-1)^nv_n \tag{θ}$$

我们经直接计算立即得到：

$$2u_{m+n}=u_mv_n+u_nv_m \tag{κ₁}$$

$$v_n^2-5u_n^2=(-1)^n4 \tag{κ₂}$$

$$u_n^2-u_{n-1}u_{n+1}=(-1)^{n-1} \tag{κ₃}$$

$$v_n^2-v_{n-1}v_{n+1}=(-1)^n5 \tag{κ₄}$$

要证明上述五性质。首先，性质1°可由(κ_3)和(κ_4)及(κ_2)直接得到。或者由公式(δ)和(ζ)的一再重现而得到的。如$(u_n, u_{n+1})=(u_n, u_n+u_{n-1})=(u_n, u_{n-1})=(u_{n-2}, u_{n-1})=(u_{n-2}, u_{n-3})=\cdots=(u_1, u_2)=1$。

2° 可由(κ_2)得到。

3° 假设对于$r=1, 2, \cdots, k-1$为真。则由(κ_1)，得

$$2u_{kn}=u_nv_{(k-1)n}+u_{(k-1)n}v_n,$$

若 u_n 是奇数，由归纳法假设

$u_n|u_{(k-1)n}\Longrightarrow u_n|2u_{kn}\Longrightarrow u_n|u_{kn}$)。若$u_n$是偶数，则由性质2°知$v_n$亦为偶数，由假设$u_n|u_{(k-1)n}\Longrightarrow 2|u_{(k-1)n}\Longrightarrow 2|v_{(k-1)n}$，所以

$$u_{kn}=u_n\left(\frac{1}{2}v_{(k-1)n}\right)+u_{(k-1)n}\left(\frac{1}{2}v_n\right)\Longrightarrow u_n|u_{kn}$$

这就证明了，对一切自然数r，3°都成立。由(θ)和 r 为 0 或负数时3°亦成立。

4°　若$(m, n)=d$，则存在$r, s\in R$使得

$$rm+sn=d$$

r，s 可以是正的或负的，并由(κ_1)得

$$2u_d=u_{rm}v_{sn}+u_{sn}v_{rm} \tag{λ}$$

因此，若$(u_m, u_n)=h$，就有

$$h|u_m,\ h|u_n \Longrightarrow h|u_{rm},\ h|u_{sn} \Longrightarrow h|2u_d$$

若h是奇数，则$h|u_d$；若h是偶数，则u_m和 u_n 都是偶数，因而由2°和3°知u_{rm}，u_{sn}，v_{rm}，v_{sn} 都是偶数，因此我们可以把(λ)写成

$$u_d=u_{rm}\left(\frac{1}{2}v_{sm}\right)+u_{sn}\left(\frac{1}{2}v_{rn}\right) \tag{λ'}$$

与前面一样可得 $h|u_d$，于是在任何情况下，$h|u_d$。由 3 °知道，

$$u_d|u_m,\ u_d|u_n \Longrightarrow u_d|(u_m,\ u_n) \Longrightarrow u_d|h.$$

$$\therefore\quad h=u_d=(u_m,\ u_n)$$

5°　若$(m, n)=1$，由3°我们有

$$u_m|u_{mn},\ u_n|u_{mn}$$

由4°得$(u_m, u_n)=1$，所以

$$u_mu_n|u_{mn}$$

由3°知道，仅当$m=4(u_4=3)$或者m是一个奇素数 p 的情况下，u_m才有可能是素数，但是u_p不一定都是素数。如

$$u_{53}=53316291173=953\times55945741$$

定理7·29　任一素数p或q都整除某些斐波那契数（并且这些数目是无限的），在特殊情况

$u_{p-1}\equiv0(\mathrm{mod}\,p)$，若$p\equiv5m\pm1$；

$u_{q+1}\equiv 0(\mathrm{mod}\,q)$，若$q\equiv 5m\pm 2$。

这个定理可以用上面的知识来证明（参考Hardy，Wright《An Introduction To The Theovy of Numbers》§10·14定理180），下面用本节前面的知识来证明。

证明 因为

$$u_n=\frac{\omega^n-\overline{\omega}^n}{\omega-\overline{\omega}}=\frac{\omega^n-\overline{\omega}^n}{\sqrt{5}}$$

这里$\omega=\frac{1}{2}(1+\sqrt{5})$，$\overline{\omega}=-\frac{1}{\omega}$是$\omega$的共轭数。

若$n=p(p=5m\pm 1)$，则由(31)得

$$\omega^{p-1}\equiv 1(\mathrm{mod}\,p),\quad \overline{\omega}^{p-1}\equiv 1(\mathrm{mod}\,p)$$

$$\Longrightarrow u_{p-1}\sqrt{5}=\omega^{p-1}-\overline{\omega}^{p-1}\equiv 0(\mathrm{mod}\,p)$$

$$\Longrightarrow u_{p-1}\equiv 0(\mathrm{mod}\,p)$$

若$n=q(q=5m\pm 2)$，则由(30)得

$$\omega^{q+1}\equiv\omega\overline{\omega}\equiv -1,\quad \overline{\omega}^{q+1}\equiv\overline{\omega}\,\omega\equiv -1(\mathrm{mod}\,q)$$

$$\Longrightarrow u_{q+1}\sqrt{5}\equiv 0(\mathrm{mod}\,q)$$

$$\Longrightarrow u_{q+1}\equiv 0(\mathrm{mod}\,q)$$

应用这些知识纳肯斯曾对默森里数为素数的问题作一些探讨，他证明了下列结论：

令$r_m=\omega^{2^m}+\overline{\omega}^{2^m}$，即$r_1$，$r_2$，$r_3$，$\cdots=3,7,47,\cdots$。若$p=4n+3$为素数，它所对应的默森里数

$$M=M_p=2^p-1$$

当$r_{p-1}\equiv 0(\mathrm{mod}\,M)$时，$M_p$是素数，并且其他情况是合数。即$M_p$为素数的充要条件是：$r_{p-1}\equiv 0(\mathrm{mod}\,M_p)$（这里不证，可参考H·W定理259或华著《数论导引》第十六章§16）。

在数论中要判断所找出的很大的默森里数是否是素数一般都采用这种方法，p很大时必须借助计算机来计算。如，

$M_{2281}=2^{2281}-1$是一个687位的素数，要判断r_{2280}是否被M_{2281}整除，就必须应用计算机。

第五节　e与π的超越性

本节将证明自然对数的底e和圆周率π都是超越数。注意本节的整数都指有理整数。

定理7·30　e是无理数。

证明　在数学分析里知道

$$e=1+\frac{1}{1!}+\frac{1}{2!}+\cdots+\frac{1}{n!}+\cdots=1+\frac{1}{1!}+\cdots+\frac{1}{n!}+\frac{1}{(n+1)!}\left[1+\frac{1}{n+2}+\frac{1}{(n+2)(n+3)}+\cdots\right]$$

$$\therefore \qquad n!e=I_n+R_n \tag{37}$$

其中$I_n=n!\left(1+\frac{1}{1!}+\frac{1}{2!}+\cdots+\frac{1}{n!}\right)=2\cdot n!+3\cdot 4\cdots n+\cdots+1$是整数，而$R_n=\frac{1}{n+1}\left[1+\frac{1}{n+2}+\frac{1}{(n+2)(n+3)}+\cdots\right]$。当$n\geqslant 2$时，因为$e<3$，故有

$$0<R_n<\frac{1}{n+1}\left(1+\frac{1}{1!}+\frac{1}{2!}+\cdots\right)=\frac{e}{n+1}<1$$

若e是有理数，设$e=\frac{a}{b}$，则当$n>b$时，(37)的左边是整数，而右边不是整数，得到矛盾，故e是无理数。

为了证明π是无理数，先证明

引理　若a是一个正常数，则当n趋向无穷大时，$\frac{a^n}{n!}$趋向于0。

证明　当$n>2a$时，

$$\frac{a^n}{n!}=\frac{a}{1}\cdot\frac{a}{2}\cdots\frac{a}{2[a]+1}\cdot\frac{a}{2[a]+2}\cdots\frac{a}{n}<M\left(\frac{1}{2}\right)^{n-(2[a]+1)}$$

其中$M=\frac{a}{1}\cdot\frac{a}{2}\cdots\frac{a}{2[a]+1}$是一个正常数。容易看出，任给$\varepsilon>0$，当 n 充分大时，$M\left(\frac{1}{2}\right)^{n-(2[a]+1)}<\varepsilon$，因而$\frac{a^n}{n!}<\varepsilon$。

$$\therefore \qquad \lim_{n\to\infty}\frac{a^n}{n}=0$$

定理 7·31 π是无理数。

证明 (i) 设$f(x)$是任一$2n$次多项式，我们先证明

$$\int_0^\eta f(x)\sin x dx=\Big[F'(x)\sin x-F(x)\cos x\Big]_0^\eta \qquad (38)$$

其中$F(x)=f(x)-f^{(2)}(x)+f^{(4)}(x)+\cdots+(-1)^n f^{(2n)}(x)$。因为由分部积分法，对任一具有一次及二次的连续导数的函数$\varphi(x)$来说。

$$\int_0^\eta \varphi(x)\sin x dx=\Big[\varphi'(x)\sin x-\varphi(x)\cos x\Big]_0^\eta-\int_0^\eta \varphi^{(2)}(x)\sin x dx \qquad (39)$$

今对多项式$f(x)$连续使用(39)至$n+1$次，得

$$\int_0^\eta f(x)\sin x dx=\Big[\{f'(x)-f^{(3)}(x)+f^{(5)}(x)-\cdots+(-1)^{n-1}f^{(2n-1)}(x)+(-1)^n f^{(2n+1)}(x)\}\sin x-\{f(x)-f^{(2)}(x)+f^{(4)}(x)-\cdots+(-1)^n f^{(2n)}(x)\}\cos x\Big]_0^\eta+(-1)^{n+1}\int_0^\eta f^{(2n+2)}(x)\sin x dx$$

因为$f(x)$是$2n$次多项式，故$f^{(2n+1)}(x)=f^{(2n+2)}(x)=0$，由上式即得(38)。

在(38)中，令$\eta=\pi$，得

$$\int_0^\pi f(x)\sin x dx=F(\pi)+F(0) \qquad (40)$$

(ii) 若π是一个有理数，设$\pi=\frac{a}{b}$，今证明可选取适当的$f(x)$使(40)不成立。如我们取

$$f(x)=\frac{x^n(a-bx)^n}{n!} \tag{41}$$

其中n是满足条件

$$\frac{\pi^{n+1}a^n}{n!}<1 \tag{42}$$

的正整数，由引理知，这种n是存在的。则$f(x)$有下列性质：

1° $f(x)$，$f'(x)$，…，$f^{(n-1)}(x)$当$x=0$，$\frac{a}{b}$时都等于0；

2° $f^{(n)}(x)$，$f^{(n+1)}(x)$，…，$f^{(2n)}(x)$都是整系数多项式，且当$x=0$，$\frac{a}{b}$时是整数。

要证1°，首先我们由(41)可以看出$f(x)$的每一项的次数$\geqslant n$，因此$f^{(j)}(x)(j=0, 1, \cdots, n-1)$都是没有常数项的多项式。故$f^{(j)}(0)=0$。又因$f\left(\frac{a}{b}-x\right)=\left(\frac{a}{b}-x\right)^n(bx)^n/n!=x^n(a-bx)^n/n!=f(x)$，所以$f^{(j)}\left(\frac{a}{b}-x\right)=f^{(j)}(x)$，从而得$f^{(j)}\left(\frac{a}{b}\right)=0$。

要证2°，观察x^k的$n+s$次导数，当$k<n+s$时，x^k的$n+s$次导数是0；当$k\geqslant n+s$，$s\geqslant 0$时，x^k的$n+s$次导数是

$$k(k-1)\cdots(k-(n+s)+1)x^{k-(n+s)} \tag{43}$$

由于C_k^{n+s}是整数，故(43)的系数是$(n+s)!$的倍数，因而是

n！的倍数。所以 $f^{(j)}(x)(j\geqslant n)$ 是整系数多项式，于是 $f^{(j)}(0)$ 是整数，又 $f^{(j)}(x)=f^{(j)}\left(\frac{a}{b}-x\right)$，故 $f^{(j)}\left(\frac{a}{b}\right)$ 也是整数。

由1°，2°立刻知道 $F\left(\frac{a}{b}\right)+F(0)$ 是整数。另一方面，当 $0<x<\frac{a}{b}=\pi$ 时，

$$0<f(x)\sin x<\frac{\pi^n a^n}{n!} \tag{44}$$

故由(40) $F(\pi)+F(0)$ 是正整数，即 $F(\pi)+F(0)\geqslant 1$。但由(44)及(42)

$$\int_0^\pi f(x)\sin x dx<\frac{\pi^{n+1}a^n}{n!}<1$$

这与(40)矛盾，故 π 不能是有理数。

定理 7·32 e是超越数。

证明 (i) 当 $f(x)$ 是任一n次多项式时，我们可以用分部积分法证明

$$F(b)=e^bF(0)-e^b\int_0^b f(x)e^{-x}dx \tag{45}$$

其中

$$F(x)=f(x)+f'(x)+\cdots+f^{(n)}(x) \tag{46}$$

事实上，由分部积分法，对任一有连续导数的函数 $\varphi(x)$ 来说，

$$\int_0^b \varphi(x)e^{-x}dx=-\left[\varphi(x)e^{-x}\right]_0^b+\int_0^b\varphi'(x)e^{-x}dx \tag{47}$$

今对多项式 $f(x)$，继续应用(47) $n+1$ 次后，得

$$\int_0^b f(x)e^{-x}dx=-\left[\{f(x)+f'(x)+\cdots+f^{(n)}(x)\}e^{-x}\right]_0^b+\int_0^b f^{(n+1)}(x)e^{-x}dx$$

由于$f(x)$是n次多项式，故$f^{(n+1)}(x)=0$，因而

$$\int_0^b f(x)e^{-x}dx=-\left[e^{-x}F(x)\right]_0^b=-e^{-b}F(b)+F(0)$$

故(45)得证。

(ii) 若e是代数数，则e是某一整系数多项式

$g(x)=c_m x^m+c_{m-1}x^{m-1}+\cdots+c_0\ (c_0\neq 0)$

的根。由(45)得

$$\sum_{k=0}^{m} c_k F(k)=F(0)\sum_{k=0}^{m} c_k e^k-\sum_{k=0}^{m} c_k e^k\int_0^k f(x)e^{-x}dx$$

$$=-\sum_{k=0}^{m} c_k e^k\int_0^k f(x)e^{-x}dx \qquad (48)$$

因此只须证明选取适当的$f(x)$之后，(48)不成立就可以了。

(iii) 令

$$f(x)=\frac{1}{(p-1)!}x^{p-1}(x-1)^p\cdots(x-m)^p$$

其中p是大于m及c_0的素数，则$f(x)$具有下列性质：

1° $f(x)$，$f'(x)$，…，$f^{(p-1)}(x)$，当$x=1$，2，…，m时，都等于0；

2° $f^{(p)}(x)$，$f^{(p+1)}(x)$，…，$f^{((m+1)p-1)}(x)$各多项式的系数都是整数，并且可以被p整除。

由于$(x-h)^p|f(x)(h=1,2,\cdots,m)$，故$f(x),f'(x),\cdots,f^{(p-1)}(x)$都被$x-h$所整除，因而$f(x)$有性质1°。

要证2°，研究x^k的$p+s$次导数，当$k<p+s$时，其导数是0；当$k\geqslant p+s(s\geqslant 0)$时，其导数是

$$k(k-1)\cdots(k-(p+s)+1)x^{k-(p+s)}$$

其系数是$(p+s)!$的倍数，因而是$(p-1)!$的倍数及p的倍数。这就证明了2°。

从$1°$及$2°$知道

$$F(1),\ F(2),\ \cdots,\ F(m)$$

都是整数，并且都是p的倍数。而

$$F(0)=f(0)+f'(0)+\cdots+f^{(p-2)}(0)+f^{(p-1)}(0)+$$
$$+f^{(p)}(0)+\cdots+f^{((m+1)p-1)}(0)$$

其中右端前$p-1$项都是0（因为$f(x)$的各项次数都不低于$p-1$），$p+1$项以后都是p的倍数，而$f^{(p-1)}(0)$是$\frac{((-1)^m m!)^p x^{p-1}}{(p-1)!}$的第$p-1$级导数，即

$$f^{(p-1)}(0)=((-1)^m m!)^p$$

$$\therefore\quad F(0)\equiv((-1)^m m!)^p(\bmod p),$$

$$\sum_{k=0}^{m} c_k F(k)\equiv c_0 F(0)\equiv((-1)^m m!)^p c_0(\bmod p)$$

但$p>m$，$p>c_0$且p是素数$\Longrightarrow p\nmid((-1)^m m!)^p c_0$，

$$\therefore\quad \sum_{k=0}^{m} c_k F(k)\not\equiv 0(\bmod p) \tag{49}$$

下面要证明，当p充分大时，

$$\left|-\sum_{k=0}^{m} c_k e^k\int_0^k f(x)e^{-x}dx\right|<1 \tag{50}$$

当x从0变到m时，$f(x)$的每一个因数$x-h$，$h=0, 1, \cdots, m$的绝对值都不超过m，因此

$$|f(x)|\leqslant\frac{1}{(p-1)!}m^{(m+1)p-1},\quad 0\leqslant x\leqslant m$$

故由积分性质得，当$0\leqslant k\leqslant m$时，

$$\left|\int_0^k f(x)e^{-x}dx\right|\leqslant\int_0^k|f(x)|e^{-x}dx\leqslant\frac{m^{(m+1)p-1}}{(p-1)!}\int_0^k e^{-x}dx$$

$$< \frac{m^{(m+1)p-1}}{(p-1)!}$$

令 $M = |c_0| + |c_1| + \cdots + |c_m|$，则

$$\left|\sum_{k=0}^{m} c_k e^k \int_0^k f(x)e^{-x}dx\right| \leqslant \sum_{k=0}^{m} \left|c_k e^k \int_0^k f(x)e^{-x}dx\right|$$

$$< \left(\sum_{k=0}^{m} |c_k|\right)e^m \frac{m^{(m+1)p-1}}{(p-1)!} = Me^m \frac{m^{(m+1)p-1}}{(p-1)!}$$

由引理知

$$\lim_{p\to\infty} Me^m \frac{m^{(m+1)p-1}}{(p-1)!} = 0$$

故p充分大时(50)成立，由(49)，(50)知(48)不成立，故 e 是超越数。

π 是超越数的证明与 e 是超越数的证明十分相似，不过更复杂而已，为了证明π 是超越数先证明

引理 设整系数多项式

$$ax^m + a_1x^{m-1} + \cdots + a_m = 0 (a \neq 0,\ m \geqslant 1) \qquad (51)$$

的根是ω_1，ω_2，…，ω_m，而α_1，α_2，…，α_n代表

$$\omega_1,\ \omega_2,\ \cdots,\ \omega_m,\ \omega_1+\omega_2,\ \omega_1+\omega_3,\ \cdots,\ \omega_{m-1}+\omega_m,\ \cdots,\ \omega_1+\omega_2+\cdots+\omega_m. \qquad (52)$$

中所有不等于 0 的数，则$a\alpha_1$，$a\alpha_2$，…，$a\alpha_n$的每一整系数对称多项式是整数。

证明 (52)中共有

$$C_m^1 + C_m^2 + \cdots + C_m^m = 2^m - 1$$

个数，今以

$$\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n,\ \alpha_{n+1},\ \cdots, \alpha_{2^m-1} \qquad (53)$$

表示它们，则$\alpha_{n+1} = \cdots = \alpha_{2^m-1} = 0$。设 $f(a\alpha_1,\ \cdots,\ a\alpha_n)$

是 $a\alpha_1$, …, $a\alpha_n$ 的任一整系数对称多项式，则由对称多项式的基本定理知，$f(a\alpha_1, \cdots, a\alpha_n)$能表成$a\alpha_1$, …, $a\alpha_n$ 的初等对称多项式的整系数多项式，而 $a\alpha_1$, …, $a\alpha_n$ 的初等对称多项式即为$a\alpha_1$, …, $a\alpha_n$, $a\alpha_{n+1}$, …, $a\alpha_{2^m-1}$的初等对称多项式，因而是 $a\omega_1$, $a\omega_2$, …, $a\omega_m$ 的对称多项式。故$f(a\alpha_1, \cdots, a\alpha_n)$能表成

$$\sigma_1 = \sum_{i=1}^{m} a\omega_i,\quad \sigma_2 = \sum_{i \neq j} (a\omega_i)(a\omega_j),\quad \cdots,\quad \sigma_m = (a\omega_1)$$

$\cdots(a\omega_m)$的整系数多项式。但 $\sigma_1 = -a_1$, $\sigma_2 = aa_2$, …
$\sigma_m = (-1)^m a^{m-1} a_m$都是整数，故$f(a\alpha_1, \cdots, a\alpha_m)$是整数。

定理 7·33 π 是超越数。

证明 (i) 若π是代数数，则存在$d_0, d_1, \cdots, d_{m'} \in R$，$d_0 \neq 0$ 使得

$$d_0\pi^{m'} + d_1\pi^{m'-1} + \cdots + d_{m'} = 0$$

两边同乘以 $i^{m'}$得

$$\{d_0(i\pi)^{m'} - d_2(i\pi)^{m'-2} + \cdots\} + i\{d_1(i\pi)^{m'-1} - d_3(i\pi)^{m'-3} + \cdots\} = 0$$

即

$$\{d_0(i\pi)^{m'} - d_2(i\pi)^{m'-2} + \cdots\}^2 + \{d_1(i\pi)^{m'-1} - d_3(i\pi)^{m'-3} + \cdots\}^2 = 0$$

因为$d_0^2 \neq 0$，故上式左边是$i\pi$的 $2m$次整系数多项式，因而$i\pi$是一个代数数，如果$i\pi$所满足的整系数既约多项式是

$$ax^m + a_1x^{m-1} + \cdots + a_m,\quad a > 0$$

其根为$\omega_1 = i\pi$, ω_2, …, ω_m。由于$1 + e^{\omega_1} = 1 + e^{i\pi} = 0$，故

$$(1 + e^{\omega_1})(1 + e^{\omega_2})\cdots(1 + e^{\omega_m}) = 0$$

左边展开即得

$$C+\sum_{k=1}^{n} e^{\alpha_k}=0,\ C>0 \tag{54}$$

其中 α_1, α_2, …, α_n 即为引理所定义的各数，而 $C-1$ 是(52)中等于 0 的数的个数。

(ii) 设$f(x)$是任一 l 次多项式，由于e^{-x}及$f(x)$在整个复数平面上解析，故(45) 式对 $\alpha_k(k=1, 2, \cdots, n)$ 仍然成立。即

$$F(\alpha_k)=e^{\alpha_k}F(0)-e^{\alpha_k}\int_0^{\alpha_k} f(x)e^{-x}dx$$

其中$F(x)=f(x)+f'(x)+\cdots+f^{(l)}(x)$，积分路线可取 0 到$\alpha_k$的直线，由(54)即得

$$CF(0)+F(\alpha_1)+\cdots+F(\alpha_k)=-\sum_{k=1}^{n} e^{\alpha_k}\int_0^{\alpha_k} f(x)e^{-x}dx \tag{55}$$

现在只要证明经过适当选择$f(x)$之后，(55)不成立就够了。

(iii) 令

$$f(x)=\frac{1}{(p-1)!}(ax)^{p-1}\{(ax-a\alpha_1)(ax-a\alpha_2)\cdots(ax-a\alpha_n)\}^p$$

其中 $p>\max(a, C, |a^n\alpha_1\alpha_2\cdots\alpha_n|)$，由引理知 $(p-1)!f(x)$是ax的整系数多项式，与定理7·32的证明一样，可证$f(x)$具有下列性质：

1° $f(x)$, $f'(x)$, …, $f^{(p-1)}(x)$当$x=\alpha_1$, α_2, …, α_n时都等于 0；

2° $f^{(p)}(x)$, $f^{(p+1)}(x)$, …, $f^{((n+1)p-1)}(x)$ 都是ax的整系数多项式，并且这些系数都被p整除。

由1°得

$$F(\alpha_k)=f^{(p)}(\alpha_k)+f^{(p+1)}(\alpha_k)+\cdots+f^{((n+1)p-1)}(\alpha_k)$$

由2°，$F(\alpha_k)$可以写成$a\alpha_k$的整系数多项式，并且系数都是p的倍数，即

$$F(\alpha_k)=p\sum_{t=0}^{np-1}b_t(a\alpha_k)^t$$

$$\therefore\quad F(\alpha_1)+F(\alpha_2)+\cdots+F(\alpha_k)=p\sum_{t=0}^{np-1}b_t\left(\sum_{k=1}^{n}(a\alpha_k)^t\right)$$

由引理知 $\sum_{k=1}^{n}(a\alpha_k)^t(t=0,1,\cdots,np-1)$都是整数。故

$\sum_{k=1}^{n}F(\alpha_k)$是整数，且

$$\sum_{k=1}^{n}F(\alpha_k)\equiv0(\bmod p)$$

依照定理7·32的证明，也可以得到 $F(0)\equiv(-1)^{pn}a^{p-1}(a\alpha_1\cdot a\alpha_2\cdots a\alpha_n)^p(\bmod p)$。故

$CF(0)+F(\alpha_1)+\cdots+F(\alpha_n)\equiv Ca^{p-1}\{(-1)^n a\alpha_1\cdot a\alpha_2\cdots a\alpha_n\}^p(\bmod p)$ 但 $p>\max(a, C, |a\alpha_1\cdot a\alpha_2\cdots a\alpha_n|)$，因此

$$(p, a)=(p, C)=(p, a\alpha_1\cdot a\alpha_2\cdots a\alpha_n)=1$$

$$\Longrightarrow p\nmid Ca^{p-1}\{(-1)^n a\alpha_1\cdot a\alpha_2\cdots a\alpha_n\}^p$$

$$\Longrightarrow CF(0)+F(\alpha_1)+\cdots+F(\alpha_n)\not\equiv0(\bmod p)\qquad(56)$$

另一方面，设$M=\max(|\alpha_1|, |\alpha_2|, \cdots, |\alpha_n|)$，则当$|x|\leqslant M$时，

$$|f(x)|\leqslant\frac{|a|^{(n+1)p-1}M^{p-1}(2M)^{np}}{(p-1)!},\quad |e^{-x}|\leqslant|e^{x}|\leqslant e^{M}$$

$$\therefore \quad \left|\int_0^{\alpha_k} f(x)e^{-x}dx\right| \leqslant \frac{2^{np}a^{(n+1)p-1}M^{(n+1)p}}{(p-1)!}e^M,$$

因积分路线的长是$|\alpha_k|\leqslant M$。由此得

$$\left|\sum_{k=1}^{n} e^{\alpha_k}\int_0^{\alpha_k} f(x)e^{-x}dx\right| \leqslant 2^{np}a^{(n+1)p-1}ne^{2M}\frac{M^{(n+1)p}}{(p-1)!}$$

由定理7·31前面的引理知道，当$p\to\infty$时，上式趋近于0，即当p充分大时

$$\left|\sum_{k=1}^{n} e^{\alpha_k}\int_0^{\alpha_k} f(x)e^{-x}dx\right| < 1 \tag{57}$$

由(56)，(57)知(55)不成立。故π是超越数。

系 $\sqrt{\pi}$是超越数

证明 若$\sqrt{\pi}$是代数数，由于代数数与代数数之积仍是代数数，故$\sqrt{\pi}\sqrt{\pi}=\pi$是代数数，这与定理7·33矛盾。

至此，我们解决了“化圆为方”问题是属于规尺作图不能问题。关于“规尺作图问题”我们把它作为本章的附录，供读者参考。

在1900年希尔伯特（Hilbert）曾提出下面的问题：当β是代数数而不是有理数，α是代数数而不等于0与1时，α^β是否一定是超越数这样一个问题。他当时认为这个问题比费马问题还要困难。但在1934年盖尔冯德（Гельфонд）与史耐得(Schneider)互相独立地证明了α^β的超越性。由此推得$e^\pi=(-1)^{-i}$是超越数。

根据现代的知识，除了上述结果之外，我们还可以证明：

$$\sin 1,\ \ln 2,\ \frac{\ln 3}{\ln 2}$$

是超越数。但是我们还不知道在α^e，α^π，π^e及欧拉常数

$\gamma\left[\gamma=\lim\limits_{n\to\infty}\left(1+\frac{1}{2}+\cdots+\frac{1}{n}-\ln n\right)\right]$之中那些是超越数，甚至不知道$\gamma$是不是无理数。

习　题

1. 证明$\xi=[1,\ 10,\ 10^{2!},\ \cdots 10^{n!},\ \cdots]$是，一个超越数。

2. 若α是一个代数数，则必有一个自然数q，使αq是代数整数。

3. 若在n次代数数域$K(\xi)$中定义：θ，$\theta^{-1}\in K(\xi)$且都是代数整数，则称θ为单位。

证明：θ为单位的充要条件是：θ是一个首项系数为1，末项系数为± 1的多项式的根。

4. 证明：任一高斯整数$a+bi$，a，$b\in R$，都是二次整数；并且全体高斯整数的集合$R[i]$是一个数环。若有理整数为系数的多项式是

$\xi=f(\alpha,\ \beta,\ \cdots,\ \gamma)$，$\alpha$，$\beta$，$\cdots$，$\gamma\in R[i]$则$\xi$亦是高斯整数。

5. 设$\rho=e^{\frac{2}{3}\pi i}=\frac{1}{2}(-1+i\sqrt{3})$，则

1° ρ是二次整数；

2° $a+b\rho=a-b-b\rho^2$，$a+b\rho^2=a-b-b\rho$，a，$b\in R$；

3° $R[\rho]$是一切形如$a+b\rho$（或$a+b\rho^2$）a，$b\in R$的复数$R[\rho]$是一个二次整数环，它与$R[\sqrt{-3}]$一致。

4° 若$\xi=a+b\rho$，则$N(\xi)=|(a+b\rho)(a+b\rho^2)|$；

5° $R[\rho]$的单位是：± 1，$\pm\rho$，$\pm\rho^2$；

6° 任给α，$\beta\in R[\rho]$，$\beta\neq 0$，存在δ，，$\gamma\in R[\rho]$使得
$\alpha=\beta\delta+\gamma$，$N(\gamma)<N(\beta)$；

7° $\lambda=1-\rho$是一个素数，3和λ^2相伴；

8° 凡具有形式$3n+1$的素数p，都可以表成a^2-ab+b^2形的数。

9° $R[\rho]$的素数是：

（i） $1-\rho$和它的相伴数；

（ii） $3n+2$形的有理素数和它的相伴数；

（iii） $3n+1$形有理素数的因数$a+b\rho$。

10° 用λ为模对$R[\rho]$进行分类有且只有三类$\{-1\}$，$\{0\}$，$\{1\}$。

6. 若有理整数$N>1$不含另一有理整数$n>1$的m次幂的因数，则$\sqrt[m]{N}$是无理数。

7. 若x_0是有理整数为系数的方程

$$x^m+c_1x^{m-1}+\cdots+c_{m-1}x+c_m=0 \tag{1}$$

的实根，则x_0是有理整数或无理数。

8. 证明：$x=\sqrt{2}+\sqrt{3}$是无理数。

9. 证明：$\lg 2$是无理数；更一般地 $\log_n m$是无理数，其中 m，$n\in R$，$n>0$且$m\neq n^t$（$t=0$，±1，±2，…）。

10. 对任一不等于 0 的有理数y，e^y是无理数。

11. π^2是无理数。

12. $\sin 1$是无理数。

13. 证明$\dfrac{\ln 3}{\ln 2}$是无理数。

14. 用盖尔冯德方法的结果证明，$\dfrac{\ln 3}{\ln 2}$是超越数。

15. 若p是形如$4n+3$的素数，且其相应的默森里数

$$M=M_p=2^p-1$$

当M是素数时，必有

$$r_{p-1}\equiv 0\ (\bmod M) \tag{1}$$

其中$r_{p-1}=\omega^{2^{p-1}}+\bar{\omega}^{2^{p-1}}$（$\omega=\frac{1}{2}+\frac{1}{2}\sqrt{5}$）。

附录Ⅱ：规尺作图问题

用圆规和无刻度的直尺（下简称规尺）来三等分任意角、化圆为方、求体积为2的立方体边长，这些著名的规尺作图问题的不可能性，是前人早已证明了的。可是，目前还有不少同志误认为这是历史上遗留的难题，而浪费时间去“解决”它，这必然是徒劳无功的。下面谈四个问题：

一、什么是规尺作图问题？

几何的作图题实际是具有某些条件的几何图形存在定理的一种变态。存在定理是断言这个几何图形是存在的，而作图题虽则是证明它确实存在的一种方法，但它并不是唯一的方法。例如，任意角的三等分线是存在的，但不能用规尺作图来求得。

在初等几何中，所谓作图题，只允许用圆规和无刻度的直尺根据作图公法，经过有限步骤作出所要求的几何图形。某些由直线和圆弧所围成的几何图形．尽管客观上是存在的，但却不能按照几何作图题的要求来作出，这样的问题就是所谓规尺作图不能问题，或简称作图不能问题。“三等分任意角”、“方圆问题”、“倍立方问题”都是著名的作图不能问题。遗憾的是，至今还有人不了解几何作图的意义，浪费时间去钻“三等分任意角”的牛角尖，有时用“制图”代替作图，还以为自己的画法是一个“突破”．“制图”与“作图”不同的地方，表现在：

1° “制图”是根据实际问题的需要，只要求作出误差甚小的，近似的几何图形；而“作图”则要求从理论上可以画出十分精确的，毫无误差的几何图形。

2° “作图”只允许有限次地使用规尺，根据几何作图

的公法来画出所要求的几何图形；而“制图”对工具不加限制，即允许用规尺之外的其他工具，如丁字尺、三角板和量角器等等，且它们的用法不受几何作图公法的限制。

例如，过任一直角三角形 ABC（如图 1）的顶点 A 作 BC的平行线 l，用圆规在直尺上，截取 DE＝2AB，移动直尺使尺边通过B点，并且使D点落在AC上，E点落在 l 上，则直线BDE就是∠ABC的三等分线之一。其证明十分简单（读者可按图 1 中的“标号”来完成）。

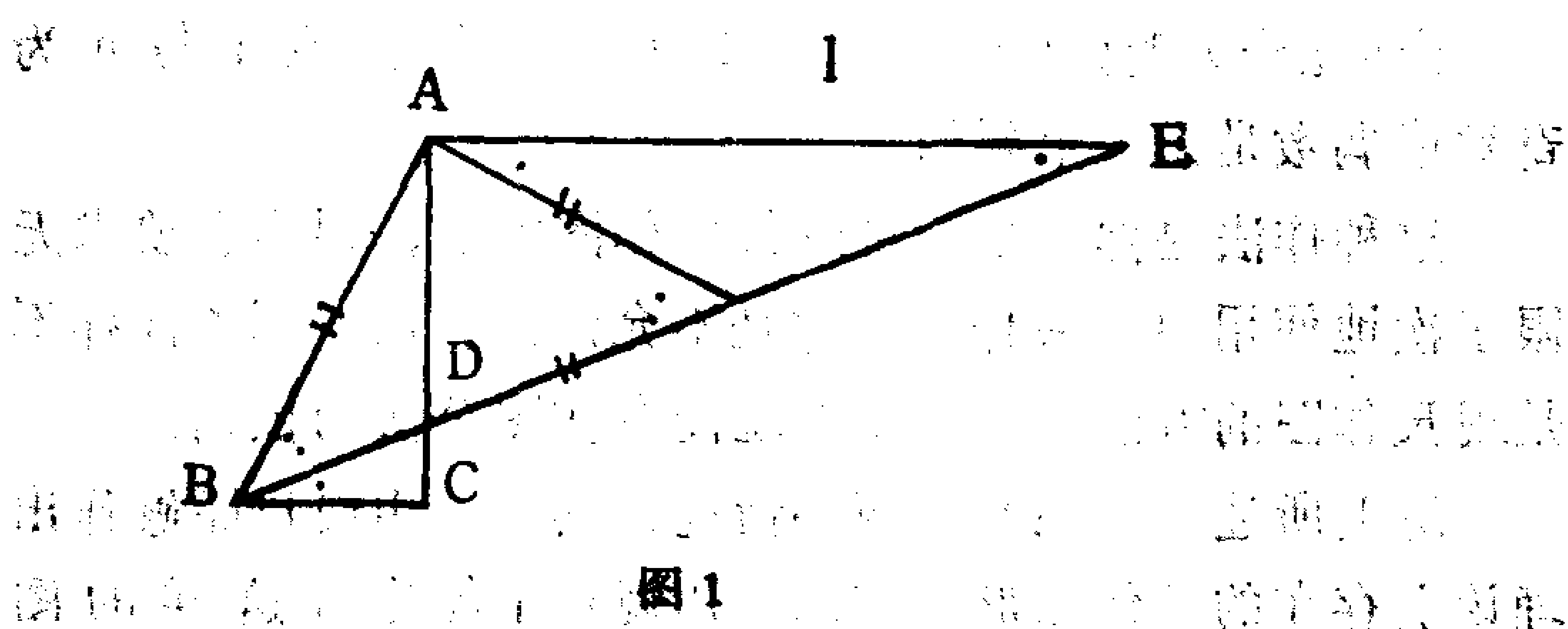


图 1

又如，在图 2 中作∠ABC的平分线BD_1，作$\angle CBD_1$的平分线 BD_2，作$\angle D_1BD_2$的平分线 BD_3，……，作$\angle D_{n-2}BD_{n-1}$的平方线D_n（n为偶数）。

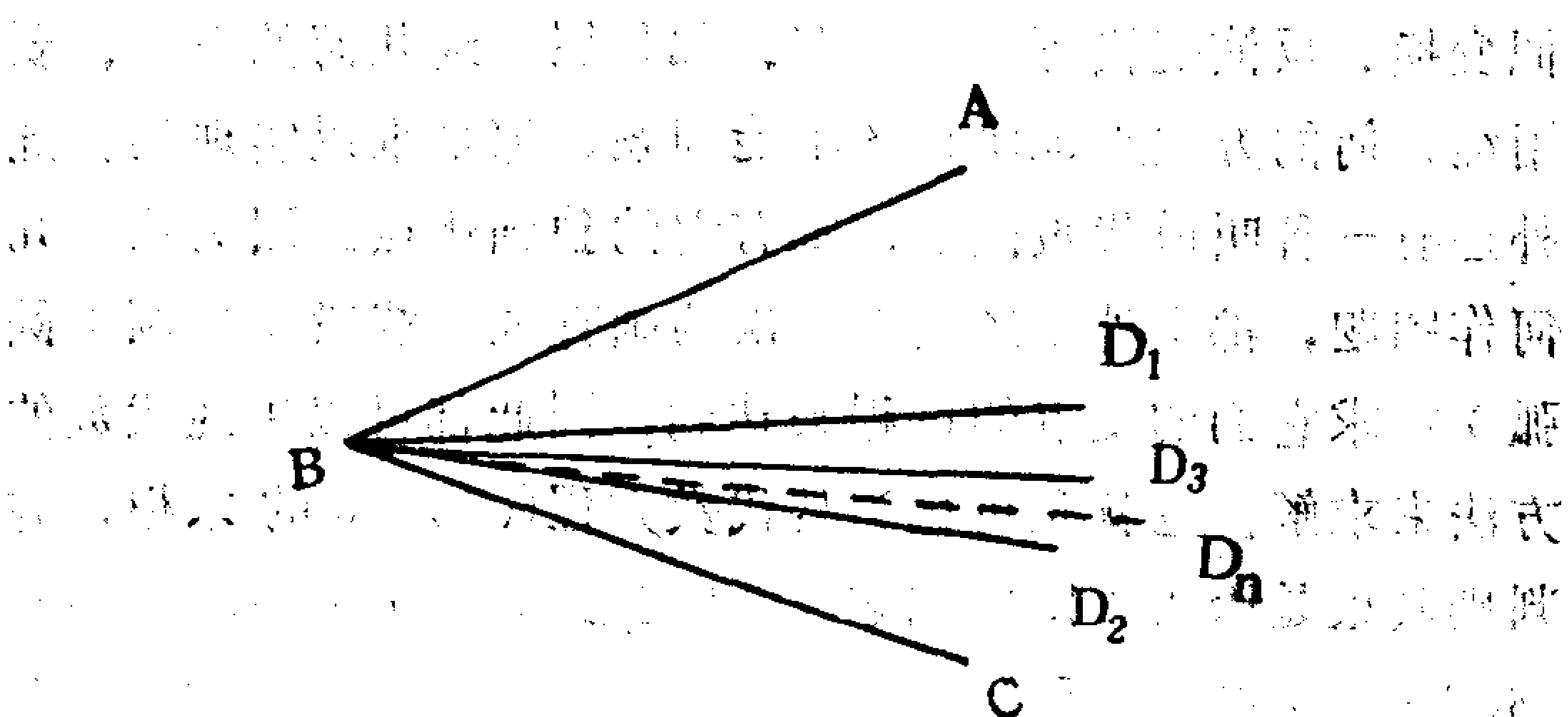


图 2

容易证明，当$n\to\infty$时，$\angle CBD_n\to\frac{1}{3}\angle CBA$。事实上，

$$\begin{aligned}\angle CBD_n &= \angle CBD_2+\angle D_2BD_4+\angle D_4BD_6+\cdots\\&\quad+\angle D_{2m-2}BD_{2m}\\&=\angle CBA\left(\frac{1}{2^2}+\frac{1}{2^4}+\frac{1}{2^6}+\cdots+\frac{1}{2^{2m}}\right)\end{aligned}$$

$$(2m=n)$$

$$\therefore\quad \lim_{n\to\infty}\angle CBD_n=\frac{1}{3}\angle CBA.$$

当n充分大时$\angle CBD_n=\angle CBD_{n+1}$，所以实际上与 n 为奇数或偶数是无关紧要的。

这种作法显然仅是一种近似的作图方法，因为它要求无限多次地使用规尺来作图，这是不允许的。前一例子同样不是规尺作图的方法，“移动”就没有作图公法为依据。

综上所述，可能产生两种情况：其一，用规尺能够作出理论上存在的几何图形；其二，用规尺不能作出这样的图形，后一种即所谓作图不能问题。

二、证明作图不能问题的途径

不管是用轨迹交截法、奠基法、变换法（合同变换、位似变换、反演变换等）来作图。都是属于纯几何的方法。要用纯几何的方法来证明作图不能问题，那是难以实现的。此外还有一种叫做代数法的，都有它的独到优点。因为任一几何作图题，都不外乎经过有限次的画直线（线段）作圆（圆弧）或求它们的交点的过程来达到，因此都可以用纯代数的方法来求解。也就是可化为某代数方程$f(x)=0$的求根，并判别其根是否可作图的问题。自从迦罗华（Galois，1811—1832）理论产生之后，已经得到了规尺作图问题的“能”与“不能”的一般判别法。

例如，著名的"倍立方"问题，就是求 $x^3-2=0$ 的正实根 $\sqrt[3]{2}$ 在数轴上的对应点；"化圆为方"问题，就是求 $x^2-\pi=0$ 的正实根 $\sqrt{\pi}$ 在数轴上的对应点等等。$\sqrt[3]{2}$ 和 $\sqrt{\pi}$ 都是不能用规尺作图的代数量，在定理 33 系中已知，$\sqrt{\pi}$ 是超越数，所以不是规尺能作图所能画出它在数轴上的对应点的，所以"化圆为方"是规尺作图不能问题。这个问题早在1882年林德曼已经证明了，它登载在1882年的"Math. Ann."（数学年报）里。$\sqrt[3]{2}$ 为什么不能作图，将在下文里证明。

一般地说，用代数法解作图题，所列方程的系数都应该是可作图的代数量（如，给定的线段长，圆弧长，定角的大小，有理数，或有理经有限次的加、减、乘、除（0不作除数）的结果，以及有理数的平方根等等），从而研究该方程的根是否仍为可作图的代数量。就是该根是否可由有限次地用画直线和圆，以及求二直线或一直线和一圆或两圆的交点等方法，来画出题目所要求的几何图形。

要求二直线的交点，就是解下列方程组：

$$\begin{cases} a_1x+b_1y+c_1=0 \\ a_2x+b_2y+c_2=0 \end{cases} \qquad (1)$$

经过消元，实质就是解x或y的一次方程，由于(1)的系数是可作图的，解之所得的根（两直线的交点）也是可作图的。因为它是可作图的代数量的有限次的加、减、乘、除的结果。

求直线和圆的交点，即解下列方程组：

$$\begin{cases} ax+by+c=0 \\ (x-\alpha)^2+(y-\beta)^2=\rho^2 \end{cases} \qquad (2)$$

求两圆的交点，即解下列方程组：

$$\begin{cases}(x-\alpha_1)^2+(y-\beta_1)^2=\rho_1{}^2 \\ (x-\alpha_2)^2+(y-\beta_2)^2=\rho_2{}^2\end{cases} \qquad (3)$$

（2）或（3）经过消元都是解一些x或y的二次方程．由于（2）或（3）的交点是可作图的，所以这些二次方程的根（实根或复根）是可作图的．这些实根或复根的实部和虚部，都是可作图量的有限次加、减、乘、除的结果．

综合上述，我们证明了，可作图的代数量只能由一次或二次方程的解得出．反之，一个可作图的代数量为系数的一次或二次方程的根，都是可作图的代数量．事实上，这些方程的根不过是它的系数（几个复数）经有限次的加、减、乘、除和开平方运算的结果．首先看复数的加、减．设$z_1=a_1+b_1i$，$z_2=a_2+b_2i$，则

$$z_1 \pm z_2=(a_1 \pm a_2)+(b_1 \pm b_2)i$$

显然$a_1 \pm a_2$和$b_1 \pm b_2$是可作图的，所以$z_1 \pm z_2$亦可作图．

其次，再看复数的乘、除法，这时可用复数的三角表示式：若

$$z_1=r_1(\cos\theta+i\sin\theta_1),\quad z_2=r_2(\cos\theta_2+i\sin\theta_2)$$

则

$$z_1z_2=r_1r_2\,[\cos(\theta_1+\theta_2)+i\sin(\theta_1+\theta_2)]$$

$$\frac{z_1}{z_2}=\frac{r_1}{r_2}\,[\cos(\theta_1-\theta_2)+i\sin(\theta_1+\theta_2)] \quad (z_2\neq0)$$

代数量r_1r_2，$\frac{r_1}{r_2}$，$\theta_1+\theta_2$，$\theta_1-\theta_2$以及$\cos(\theta_1+\theta_2)$，$\cos(\theta_1-\theta_2)$，$\sin(\theta_1+\theta_2)$，$\sin(\theta_1-\theta_2)$都可以作图，所以z_1z_2和$\frac{z_1}{z_2}$也是可作图的．

最后，$z=r(\cos\theta+i\sin\theta)$的平方根

$$z^{\frac{1}{2}}=r^{\frac{1}{2}}\left(\cos\frac{\theta}{2}+i\sin\frac{\theta}{2}\right)$$

$\sqrt{r}$ 和二等分任意角以及已知解的正弦、余弦函数都是可作图的，故$z^{\frac{1}{2}}$可作图。

上面的讨论，已经证明了

定理 1 一个代数量能用规尺作图的充分且必要条件是：这个代数量仅能是一些可作图代数量为系数的，次数不高于二的方程的求解的结果（根）。

这个定理的意义是：一个可作图的代数量α，一定是另一些可作图代数量 a，b，c，…为系数的一次或二次方程（如，$ax^2+bx+c=0$）的根，而 a，b，c，…又是另一些可作图的代数量a'，b'，c'，…为系数的一次或二次方程的根（如，a是$a'x^2+b'x+c'=0$的根等等）。依此类推，α的作图可通过一串次数不高于二的方程的根的作图来完成。因此定理 1 指出了：

定理 1′ 代数方程$f(x)=0$的根可作图的充要条件是：方程$f(x)=0$可还原成一串次数不高于二的方程。

例如，$f(x)=x^4-2x^2-1$的一个实根$\alpha=\sqrt{1+\sqrt{2}}$，实际上是以二次方程$y^2-2y-1=0$的一个实根$\alpha=1+\sqrt{2}$为系数的二次方程$x^2=1+\sqrt{2}$的正根$\alpha=\sqrt{1+\sqrt{2}}$。也就是把方程$f(x)=0$还原成一串方程$y^2-2y-1=0$和$x^2=y_1$，其中$y_1=1+\sqrt{2}$是前一个方程的根。因此，要作出α长的线段，先作出长为y_1的线段，次作出$1:\alpha=\alpha:(1+\sqrt{2})$中的长为$\alpha$的线段。

但是定理1′还不能判别对给定的方程是不是可以还原成一串次数不高于二的方程？另一方面这一串方程的系数是属于不同的数域里，这些数域的构造怎样？如何构造？这与本

章的代数数域有关. 这些内容都是我们下面要着手解决的问题。

三、规尺作图能不能的判别法

解决规尺作图能不能问题的一般判别法应归功于青年数学家迦罗华。如果用GF(p)表示模p的剩余类{0}，{1}，…，{p-1}的集合，按照类的加、乘运算，它是一个域。在这样的域上的方程可以没有解，如，$x^2-x-1=0$ 在GF(3)上没有解。迦罗华简单地假定它有一个解存在，把j"添加"于GF(3)，得到一个扩域GF(3，j)，方程$x^2-x-1=0$在GF(3，j)中有解。这个思想被柯西（Cauchy）称为迦罗华思想。这个思想发展成迦罗华域的理论。事实上，当时迦罗华提出这个问题在逻辑推理上是很不满意的，以后由柯西给出满意的结论，建立了代数扩张(algebraic extension)、有限扩张（finite extension）的理论，把这些成就归功于迦罗华。如，$y^2-2y-1=0$ 在有理数域上无解，若把$\sqrt{2}$添加于有理数域K，得到包含一切形如$a+b\sqrt{2}$（$a, b\in K$）的集合$K(\sqrt{2})$，对通常实数的加、乘运算是一个域，即正文中的一个二次代数数域。在$K(\sqrt{2})$中该方程有解 $1+\sqrt{2}$。

GF(3，j)是一切形如 $\alpha(j)=a_0+a_1j$（$a_0=0, 1, 2$；$a_1=0, 1, 2$）元素的集合。这些元素是把以GF(3)的元素为系数的x的任意次数的多项式f(x)，用 $m(x)=x^2-x-1$ 除之，得

$$f(x)=g(x)(x^2-x-1)+r(x),\quad r(x)=a_0+a_1x$$

令$x=j$得 $f(j)=r(j)$。

也就是与求剩余类一样地，把GF(3)上x的多项式环GF(3)[x]=GF[3，x]的元素用$m(x)=x^2-x-1$为模来进行分类，这些类的集合论作GF(3,x)或GF[3，x]/{m(x)}，

取$x=j$时，就是添加j于GF(3)所得到的代数扩张，它与GF(3, x)同构（一样的）。

把迦罗域GF(p, x)的基域GF(p)换为任意域（或有理数域，或实数域）P，就引入了代数扩张的概念。代数扩张指的是：添加P上既约多项式m(x)的根α于P，所得到的扩域$P(\alpha)$，它与P上多项式环$P[x]$的元素用m(x)为模进行分类，所得的域$P[x]/\{m(x)\}$同构。

如果Ω是域P的扩域，并且在Ω中存在$u_1, u_2, \cdots, u_m$关于P线性无关，任一$u\in\Omega$，u都是$u_1, u_2, \cdots, u_m$的线性组合，这样的Ω叫做P的m次有限扩张；$u_1, u_2, \cdots, u_m$称为Ω关于P的基底，简称基底。下面将证明一切代数扩张都是有限扩张。这些概念都肇源于迦罗华思想。

例如，设Δ（下面都用Δ代替正文中的K）是有理数域，添加多项式x^2-2的根$\sqrt{2}$于Δ，得到一个代数扩张$\Delta(\sqrt{2})=\{a+b\sqrt{2}\,|\,a, b\in\Delta\}$，在$\Delta(\sqrt{2})$里可以施行一般实数的加、减、乘、除（0不作除数）运算，所以它是Δ的扩域。且它的任一数都是1，$\sqrt{2}$的线性组合，所以$\Delta(\sqrt{2})$是有理数域Δ上的二次有限扩张。一般地，任一二次代数数域，都是Δ上二次有限扩张。

因为有理数域Δ上任意次数的既约多项式都存在，设α是Δ上$m(m\geqslant 1)$次既约多项式的根，添加α于Δ得到的代数扩张$\Delta(\alpha)$是Δ的m次有限扩张。用$(\Omega:\Delta)$表示Ω关于Δ的次数（degree）。例如，$(\Delta(\sqrt{2}):\Delta)=2$；$(\Delta(\alpha):\Delta)=m$等。

1．有限扩张的构造。

定理 2 设Ω是域Δ的二次有限扩张，则Ω是由添加一个Δ上的二次既约多项式的根而得到的。

如果Ω是△上的n次有限扩张，则Ω是△上的n维线性空间。Ω关于△的基底就是该线性空间的基底，要证明定理2，用到线性空间的下列诸性质。

1° 若$(\Omega:\triangle)=n$，则Ω里关于△线性无关的元素的个数s不能大于n。

2° 若$(\Omega:\triangle)=n$，则Ω里任一组线性无关的n个元素，都是Ω的一个基底。

3° Ω关于△的次数，不随基底的选择而变化。

4° 若$\Omega:\triangle=n$，则任一$\alpha\in\Omega$都是△上次数不高于n的多项式$f(x)$的根。

证明 若$\alpha=0$，它是$x=0$的根；若$\alpha\neq0$，$\alpha\in\Omega$，则$\alpha^0=1$，$\alpha^1=\alpha$，α^2，…，α^n是Ω的$n+1$个元由1°知道它线性相关，即存在△的不全为零的元素a_0，a_1，a_2，…，a_n使得

$$a_0+a_1\alpha+a_2\alpha^2+\cdots+a_n\alpha^n=0$$

也就是α是

$$f(x)=a_nx^n+\cdots+a_1x+a_0$$

的一个根。

定理2的证明 因为$(\Omega:\triangle)=2$，所以Ω中必含有不属于△的元素，设$\alpha\in\Omega$，$\alpha\in\triangle$，由性质4°知道α是△上二次既约多项式

$$a_2x^2+a_1x+a_0\ (a_2\neq0) \tag{4}$$

的一个根。否则，如果$a_2=0$，那末$\alpha=-\frac{a_0}{a_1}\in\triangle$，这与$\alpha\in\triangle$矛盾；如果$a_2x^2+a_1x+a_0=(b_1x+c_1)(b_2x+c_2)$ $(b_1,\ b_2,\ c_1,\ c_2\in\triangle)$，那末$\alpha=-\frac{c_1}{b_1}$或$\alpha=-\frac{c_2}{b_2}$都属于△，亦与$\alpha\in\triangle$的假设矛盾。

今证明 1，α 是Ω的一个基底. 1，α 线性无关是显然的。由性质1°知道，任给$\beta\in\Omega$都有β，1，α线性相关，即存在$b_2\neq0$，b_1，$b_0\in\triangle$，使得

$$b_2\beta+b_1\alpha+b_0=0，\quad 或 \quad \beta=-\frac{b_1}{b_2}\alpha-\frac{b_0}{b_2}=c_1\alpha+c_0,$$

其中c_0,$c_1\in\triangle$.这就是说,Ω的任一元素都可以表成 $c_1\alpha+c_0$的形式，其中c_1，$c_0\in\triangle$。即Ω是添加(4)的根 α 于$\triangle$所得到的代数扩张$\triangle(\alpha)=\Omega$。

系 若添加域$\triangle$上的$n(n>1)$次既约多项式$p(x)$的一个根α于$\triangle$，所得到的代数扩张为$\triangle(\alpha)$，则$\triangle(\alpha)$是$\triangle$上一个次数为 n 的有限扩张。

证明 设α是$\triangle$上n次既约多项式$p(x)$的根，则1，α，α^2，…，α^{n-1}是$\triangle(\alpha)$的一个基底。

首先证明，1，α，…，α^{n-1}线性无关。否则，存在不全为零的元素b_0，b_1，…，b_{n-1}，使得

$$h(\alpha)=b_0+b_1\alpha+\cdots+b_{n-1}\alpha^{n-1}=0$$

以$h(x)$除$p(x)$得

$$p(x)=h(x)q_1(x)+r_1(x),\quad \partial r_1(x)<n-1 \qquad (5)$$

其中$\partial r_1(x)$表示$r_1(x)$的次数，若$r_1(x)=0$，则$h(x)|f(x)$，这与$f(x)$是既约的假设矛盾，故 $r_1(x)\neq0$。令 $x=\alpha$，代入(5)得$r_1(\alpha)=0$。再用$r_1(x)$除$p(x)$得

$$p(x)=r_1(x)q_2(x)+r_2(x),\quad \partial r_2(x)<n-2$$

重复上面的讨论，可得

$$p(\alpha)=h(\alpha)=r_1(\alpha)=r_2(\alpha)=\cdots=r_s(\alpha)=0$$

其中$\partial p(x)>\partial h(x)>\partial r_1(x)>\partial r_2(x)>\cdots>\partial r_s(x)=1$，这就得到了 α 是$\triangle$上一次多项式的根,$\alpha\in\triangle$,即 $(x-\alpha)|p(x)$ 这与 $p(x)$ 不可约的假设矛盾。所以当 $h(\alpha)=0$时，只能是

$b_0=b_1=\cdots=b_{n-1}=0$。

其次，任一$\beta\in\triangle(\alpha)$，则根据代数扩张元素的构造

$$\beta=b_0+b_1\alpha+\cdots+b_m\alpha^m=g(\alpha),\ b_i\in\triangle,\ b_m\neq 0$$

若$m<n$，则β是1，α，…，α^{m-1}的线性组合；若$m\geqslant n$，则用$p(x)$除$g(x)$，得

$$g(x)=p(x)q(x)+r(x),\ \partial r(x)\leqslant n-1$$

$$\therefore\quad g(\alpha)=p(\alpha)q(\alpha)+r(\alpha)=r(\alpha)$$

亦即$\beta=r(\alpha)$是1，α，…，α^{n-1}的线性组合。这就证明了1，α，…，α^{n-1}是$\triangle(\alpha)$的一个基底，故$\triangle(\alpha)$是$\triangle$的n次有限扩张。

由系，当$n=2$时，可得到定理2的逆定理。

定理 3 设Ω_1是域$\triangle$的有限扩张，Ω_2是Ω_1的有限扩张，则Ω_2是$\triangle$的有限扩张。且

$$(\Omega_2:\triangle)=(\Omega_1:\triangle)\times(\Omega_2:\Omega_1)$$

证明 根据有限扩张的定义，若$(\Omega_1:\triangle)=m$，$\Omega_2:\Omega_1=n$，则存在$\alpha_1,\alpha_2,\cdots,\alpha_m$是$\Omega_1$关于$\triangle$的基底，$\beta_1$，$\beta_2,\cdots$，$\beta_n$是$\Omega_2$关于$\Omega_1$的基底。任给$\alpha\in\Omega_2$都有

$$\alpha=\gamma_1\beta_1+\gamma_2\beta_2+\cdots+\gamma_n\beta_n=\sum_{i=1}^{n}\gamma_i\beta_i\ (\gamma_i\in\Omega_1)$$

而且

$$\gamma_i=\sum_{j=1}^{m}a_{ji}\alpha_j\ (i=1,\ 2,\ \cdots,\ n;\ a_{ji}\in\triangle)$$

$$\therefore\quad \alpha=\sum_{i=1}^{n}\left(\sum_{j=1}^{m}a_{ji}\alpha_j\right)\beta_i=\sum_{i=1}^{n}\sum_{j=1}^{m}a_{ji}(\alpha_j\beta_i)$$

其中$\alpha_j\beta_i\in\Omega_2(j=1,\ 2,\ \cdots,m;\ i=1,\ 2,\ \cdots,\ n)$。今证明

$$\alpha_1\beta_1,\ \cdots,\ \alpha_1\beta_n,\ \alpha_2\beta_1,\ \cdots,\ \alpha_2\beta_n,\ \cdots,\ \alpha_m\beta_n \quad (6)$$

关于$\triangle$线性无关，即Ω_2关于$\triangle$的基底包含有$m\times n$个线性无

关的元素，所以$(\Omega_2:\Delta)=(\Omega_1:\Delta)\cdot(\Omega_2:\Omega_1)$。事实上，任意

$$\sum_{i=1}^{n}\sum_{j=1}^{m}c_{ji}\alpha_j\beta_i=0\quad(c_{ji}\in\Delta,\ \alpha_j\in\Omega_1,\ \beta_i\in\Omega_2)$$

时，上式改写为

$$\sum_{i=1}^{n}\left(\sum_{j=1}^{m}c_{ji}\alpha_j\right)\beta_i=\sum_{i=1}^{n}\delta_i\beta_i=0\,(\delta_i\in\Omega_1)$$

由于β_1，β_2，…，β_n是Ω_2关于Ω_1线性无关的元素组，

$$\therefore\quad \delta_i=\sum_{j=1}^{m}c_{ji}\alpha_j=0\quad(i=1,\ 2,\ \cdots,\ n)$$

同理，因为α_1，α_2，…，α_m是Ω_1关于Δ的基底，

$$\therefore\quad c_{ij}=0(j=1,\ 2,\ \cdots,\ m;\ i=1,\ 2,\ \cdots,\ n)$$

这就证明了(6)是Ω_2关于Δ的一个基底，且

$$(\Omega_2:\Delta)=m\times n=(\Omega_1:\Delta)\cdot(\Omega_2:\Omega_1)$$

定理 4 设Ω是域Δ的有限扩张，且域Σ满足$\Delta\sqsubseteq\Sigma\sqsubseteq\Omega$，则$\Sigma$也是$\Delta$的有限扩张，并且$(\Sigma:\Delta)|(\Omega:\Delta)$。

证明 设$(\Omega:\Delta)=n$，即Ω关于Δ线性无关的元素组最多只包含有n个元素，由性质1°知道域Σ中必存在$m(m\leqslant n)$个元素β_1，β_2，…，β_m，它们是Σ关于Δ线性无关最大数的元素组，由性质2°知道这个元素组就是Σ关于Δ的一个基底。Σ是Δ的m次有限扩张，即$(\Sigma:\Delta)=m$。

因为$\Delta\sqsubseteq\Sigma\sqsubseteq\Omega$，设$\Omega$关于$\Sigma$的线性无关最大数的元素组包含有t个元素，与上面同样的方法，可以证明Ω是Σ的t次有限扩张。由定理3知道

$$\Omega:\Delta=(\Omega:\Sigma)\cdot(\Sigma:\Delta)=m\cdot t=n$$

$$\therefore\quad m|n$$

上面知识说明了，每一个域△上的代数扩张都是一个△上的有限扩张，反之，△上的每一个有限扩张，都可以分解成一串代数扩张。事实上，设Ω是△的n次有限扩张，若Ω中存在△上的n次既约多项式f(x)的根α时，则Ω＝△(α)为代数扩张。若Ω中含有最高次数为 m(m<n) 的既约多项式 p(x) 的根β，则添加β于△得到一个△的m次有限扩张 △(β)，并且Ω⊒△(β)，由定理 4 知道 m|n，Ω是△(β)的 $\frac{n}{m}=t$ 次有限扩张。若Ω 中含有△(β)上k(k⩽t) 次的约多项式 q(x)的根r，则△(β)(r)是△(β)的k次代数扩张，k|t。若k＝t，则Ω 可分解成两次代数扩张：Ω＝〔△(β)〕(r)＝△(β，r)；若k<t，可依此类推使 Ω＝△(β，r，…，δ) 是由一串代数扩张来表示。其中(Ω：△)＝n＝m·k…s。

2．正规域

设域△上多项式

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$$

在△内可分解成

$$f(x)=(x-\alpha_1)\cdots(x-\alpha_s)p_1(x)\cdots p_r(x)$$

其中 $p_i(x)(i=1,2,\cdots,r)$ 是△上高于一次的既约多项式。因为$\alpha_j\in\triangle(j=1,\cdots,s)$，所以添加 α_j 于△，△保持不变；但是添加$p_1(x)$的根β_1于△，所得到的$\partial p_1(x)$次的代数扩张（有限扩张）$\triangle_1=\triangle(\beta_1)$，在$\triangle_1$中f(x)可分解为

$$f(x)=(x-\alpha_1)\cdots(x-\alpha_s)(x-\beta_1)\cdots(x-\beta_i)q_1(x)\cdots q_l(x)$$

其中 $q_i(x)(i=1,\cdots,l)$ 表示$\triangle_i$上次数高于 1 的既约多项式。再添加$q_1(x)$的根γ_1于$\triangle_1$，得到$\triangle_2=\triangle_1(\gamma_1)=\triangle(\beta_1)(\gamma_1)$，依此类推，有限次后，可以得到△的扩域Ω，

在Ω里$f(x)$可分解成纯一次多项式之积，这样的$\triangle$的有限扩张Ω叫做多项式$f(x)$的正规域(normal field)。有

$$\triangle\subset\triangle_1\subset\triangle_2\subset\cdots\subset\triangle_k=\Omega$$

其中$\triangle_1$，$\triangle_2$，…，$\triangle_k$是依次添加$\triangle$，$\triangle_1$，…，$\triangle_{k-1}$上的次数高于1的既约多项式$f_0(x)=p_1(x)$，$f_1(x)=q_1(x)$，…，$f_{k-1}(x)$的根而得到的代数扩张。

由定理2的系和定理4，立即得到

定理 5 若Ω是域$\triangle$上多项式$f(x)$的正规域，$p(x)$是$f(x)$的既约因式，则$\partial p(x)\mid(\Omega:\triangle)$。

定理 6 若Ω是域$\triangle$上多项式$f(x)$的正规域，且$(\Omega:\triangle)=2^m(m>1)$，则存在$\triangle$的二次有限扩张$\triangle_1$，使得$\triangle\subset\triangle_1\subset\Omega$。

证明 如果$f(x)$在$\triangle$上可分解成纯一次多项式之积，则$(\Omega:\triangle)=1$与$(\Omega:\triangle)=2^m(m>1)$的假设矛盾。所以至少有一个$\triangle$上次数大于1的既约多项式$p(x)$存在，使得$p(x)\mid f(x)$，由定理2的系及定理5知道，$\partial p(x)=2^t(1\leqslant t\leqslant m)$。

当$t=1$时，定理已证明，因为只要把二次既约多项式$p(x)$的任一根α添加于$\triangle$得到$\triangle_1=\triangle(\alpha)$，且$(\triangle_1:\triangle)=2$，$\triangle\subset\triangle_1\subset\Omega$。

当$t>1$时，证明比较复杂，下面分两个步骤。首先，设α_1，α_2，…，α_{2^t}是$p(x)$的根，它们不属于$\triangle$，今构造一个辅助多项式

$$g(x)=\Pi(x-\beta_k)$$

其中$\beta_k=\alpha_i\alpha_j+c(\alpha_i+\alpha_j)$，$\alpha_i$，$\alpha_j$是$p(x)$的任意两个根，$c\in\triangle$，则$\partial g(x)=C_{2^t}^2=\dfrac{2^t(2^t-1)}{2}=2^{t-1}Q$（Q是奇数）.我们可以选取适当的c，使得$\beta_k(k=1,2,\cdots,2^{t-1}(2^t-1))$都

不属于△．事实上，如果这样的c不存在，那末$c_1, c_2 \in \triangle$使得

$$\alpha_i\alpha_j + c_1(\alpha_i+\alpha_j) \in \triangle,\quad \alpha_i\alpha_j + c_2(\alpha_i+\alpha_j) \in \triangle$$

令
$$\begin{cases} \alpha_i\alpha_j + c_1(\alpha_i+\alpha_j) = d_1 \\ \alpha_i\alpha_j + c_2(\alpha_i+\alpha_j) = d_2 \end{cases} \tag{7}$$

其中d_1，$d_2 \in \triangle$，解方程组（7），得

$$\left.\begin{aligned} \alpha_i+\alpha_j &= \frac{d_1-d_2}{c_1-c_2} = b_1 \\ \alpha_i\alpha_j &= \frac{d_2c_1-d_1c_2}{c_1-c_2} = b_2 \end{aligned}\right\} \quad (b_1,\ b_2 \in \triangle)$$

所以α_i，α_j是△上二次多项式$h(x)=x^2-b_1x+b_2$的二根，则$h(x)|p(x)$，这与$p(x)$在△上既约的假设矛盾。

今假设已选好了符合上述条件的c，而使辅助多项式$g(x)$的$2^{t-1}(2^t-1)$个根都不属于△，由于$g(x)$的系数都是$p(x)$的根的对称函数，所以它们都属于△。故$g(x)$是△上次数为$2^{t-1}(2^t-1)=2^{t-1}Q$（Q是奇数）的多项式。

其次，因为Ω是$f(x)$的正规域，$p(x)$的一切根都属于Ω，所以$\beta_k \in \Omega$($k=1, 2, \cdots, 2^{t-1}(2^t-1)$)，故$g(x)$的正规域是Ω的子域．又因$\beta_k \in \triangle$，所以$g(x)$在△上无一次因子。今以$g(x)$代替$f(x)$来讨论。设$p_1(x)$是$g(x)$的次数最低的△上的既约因式，则$\partial p_1(x)=2^{t_1}(1 \leqslant t_1 \leqslant t-1)$．因为添加$p_1(x)$的一个根于△得到的有限扩张$\triangle_1$，则$(\triangle_1:\triangle)|(\Omega:\triangle)$，所以$(\triangle_1:\triangle)=\partial p_1(x)=2^{t_1}(t_1 \leqslant t-1)$。

如果$t_1=1$那末定理已证明；如果$t_1>1$，那末以$\beta_k=\alpha_i\alpha_j+c(\alpha_i+\alpha_j)$代替$p_1(x)$的根，重复上面的讨论，构造辅助多项式$g_1(x)$，可得一个△上$2^{t_2}$次的既约多项式$p_2(x)$，其中$1 \leqslant t_2 \leqslant t-2$．依此类推，有限次必然可得到一个在Ω里可分解的△上二次既约多项式$p_s(x)$，添加它的根于△，

得到一个二次有限扩张Δ_1，而且

$$\Delta\subset\Delta_1\subset\Omega.$$

从这个定理可以直接推得

系 1 若域Δ上的多项式$f(x)$的正规域Ω关于Δ的次数等于$2^m(m>1)$时，则存在一串二次有限扩张Δ_1，Δ_2，…，$\Delta_m=\Omega$，其中Δ_i是$\Delta_{i-1}(i=1, 2, \cdots, m)$的二次有限扩张，使得

$$(\Omega:\Delta)=(\Omega:\Delta_{m-1})\cdot(\Delta_{m-1}:\Delta_{m-2})\cdots(\Delta_2:\Delta_1)\cdot(\Delta_1:\Delta)$$

又由定理 2 可得系 1 中的Δ_i是由添加Δ_{i-1}上的二次多项式$f_i(x)(i=1, \cdots, m)$的一个根所得到的代数扩张。

系 2 若Ω是域Δ上多项式$f(x)$的正规域，且$(\Omega:\Delta)=2^m(m>1)$，$\Delta\subset\Delta_1\subset\Delta_2\subset\cdots\subset\Delta_m=\Omega$，其中$\Delta_i$是添加$\Delta_{i-1}$上二次既约多项式$f_i(x)$的根于$\Delta_{i-1}$所得到的二次有限扩张，则$f(x)$的根是$f_0(x)$，$f_1(x)$，…，$f_{m-1}(x)$的根与$\Delta$的元素的有理式。

一般地，我们可以定义：域Δ上的多项式$f(x)$，若方程$f(x)=0$的根可由下面次数不高于二的诸方程

$$f_0(x)=0,\ f_1(x)=0,\ \cdots,\ f_s(x)=0 \qquad (8)$$

的根的有理式来表示。我们就说$f(x)=0$可还原成一串次数不高于二的方程。其中$f_0(x)$是Δ上一次或二次多项式，把$f_0(x)$的根α_0添加于Δ，得到$\Delta_1=\Delta(\alpha_0)$；而$f_1(x)$是$\Delta_1$上的一次或二次多项式，…，$f_s(x)$是$\Delta_{s-1}=\Delta_{s-2}(\alpha_{s-2})$上的一次或二次既约多项式。

3．规尺作图能不能问题的判别法

有了前面的准备工作，我们知道，有理数域Δ上的方程$f(x)=0$的根可作图的充要条件是：$f(x)=0$可还原成一串

次数不高于二的方程：$f_0(x)=0, f_1(x)=0, \cdots, f_s(x)=0$。因此，一个代数方程的根能不能用规尺作图的判别定理是：

定理 7 设Ω是域（特别是有理数域）$\triangle$上的方程$f(x)=0$的正规域，方程$f(x)=0$可还原成一串次数不高于二的方程的充要条件是：

$$(\Omega:\triangle)=2^m(m\geqslant 0)$$

定理的充分性已由定理6系2给出了，所以下面只需证明必要性。

证明 设域$\triangle$上方程$f(x)=0$，可还原为一串次数不高于二的方程

$$f_0(x)=0, \quad f_1(x)=0, \quad \cdots, \quad f_s(x)=0 \qquad (8)$$

我们把(8)中诸方程的根α_0，α_1，…，α_s依次添加于$\triangle$，$\triangle(\alpha_0)=\triangle_1$，$\triangle_1(\alpha_1)=\triangle_2$，…，$\Gamma=\triangle_s(\alpha_s)$，在有限扩张$\Gamma$中$f(x)$可分解成一次因子之积，故$\Gamma\supseteq\Omega$。当(8)中方程都是一次时，$\Omega=\Gamma=\triangle$，$(\Omega:\triangle)=1=2^0$；若不全为一次时，$(\Gamma:\triangle)=2^t$，由定理4知道$(\Omega:\triangle)|(\Gamma:\triangle)$，所以$(\Omega:\triangle)=2^m(0\leqslant m\leqslant t)$。

四、“倍立方”、三等分任意角和割圆问题

1．“倍立方”问题

“倍立方”问题亦称“立方倍积”问题。是讨论能否用规尺作出体积等于2的立方体的边长，即判别有理数域$\triangle$上既约三次多项式*

$$f(x)=x^3-2=0$$

*用爱森斯坦因（Eisenstein）判别法，易证x^3-2在有理数域上不可约，爱氏判别法指的是：假设除去a_n外，多项式

$$f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n\ (a_n\neq 0, \ n\geqslant 1, \ )$$

的每一个系数都是p的倍数，但a_0不是p^2的倍数，则$f(x)$在有理数域上是既约的。

的方程是否可还原成一串一次或二次方程．

添加 $x^3-2=0$ 的一个实根$\sqrt[3]{2}$于有理数域△所得到的有限扩张△($\sqrt[3]{2}$)，有基底 1，$\sqrt[3]{2}$，$\sqrt[3]{4}$，所以(△($\sqrt[3]{2}$)：△)＝3．

若 Ω是f(x)的正规域，(Ω：△)＝n，由定理 4 知道3|n．所以$n=2^m$．由定理 7 知道"倍立方"是规尺作图不能问题．

2．三等分任意角问题

设已知角α，把α三等分得到角φ，即 $\varphi=\frac{1}{3}\alpha$，或 $\alpha=3\varphi$，则

$$\cos\alpha=\cos3\varphi=4\cos^3\varphi-3\cos\varphi \tag{9}$$

因为已知角α可作图，故cosα亦可作图，令 $\cos\alpha=\frac{b}{2}$（$|b|\leqslant 2$），b是可作图的代数量．cosφ是未知量，令$\cos\varphi=\frac{x}{2}$，则

$$\frac{b}{2}=4\left(\frac{x}{2}\right)^3-3\cdot\frac{x}{2}$$

或者 $$f(x)=x^3-3x-b=0 \tag{10}$$

(10)中可取满足$|b|\leqslant 2$ 的b 值使(10) 在有理数域△上不可约，例如，取$b=1\left(\alpha=\frac{\pi}{3}\right)$，(10)就没有有理根了．事实上，$x^3-3x-1=0$ 若有有理根只能是±1，但f(1)＝－3，f(－1)＝1，所以$x^3-3x-1=0$ 无有理根．若添加 $f(x)=x^3-3x-1$的实根β于△，得到$\triangle_1=\triangle(\beta)$，则$(\triangle_1:\triangle)=3$，若Ω是f(x)的正规域，则 3|(Ω：△)，所以三等分 60°角是不可能的．也就是三等分任意角是规尺作图不能问题．

一般地，若$\alpha=\arccos\frac{1}{2p}$（p为素数）时，多项式

$$f(x)=x^3-3x-\frac{1}{p}$$

在有理数域上是既约的，这样的角α 都不能用规尺三等分。

事实上，令 $y=\frac{1}{x}$，则

$$g(y)=y^3+3py^2-p=0$$

在有理数域上既约，故$f(x)$在有理数域上亦既约。

3．割圆（cyclotomic）问题

高斯证明了下面的定理：

定理 8 可以用圆规和直尺把圆周n 等分的充分且必要条件是：

$$n=2^t q_1 q_2 \cdots q_s$$

式中 t 是非负整数，$q_i(i=1, 2, \cdots, s)$ 是互不相同的形如2^k+1的奇素数。

如，5等分、10等分、17等分、…圆周是可能的；而7等分、13等分、15等分、…圆周是不可能的。

要证明定理8，先证明

引理 1 设$n=n_1n_2$,$(n_1, n_2)=1$,则利用规尺可n等分圆周的充要条件是：可用规尺n_1等分圆周，且 n_2等分圆周.

证明 若用规尺可n_1，n_2等分圆周，$(n_1, n_2)=1$，则存在整数x，y使得

$$n_1x+n_2y=1, \text{或} \frac{y}{n_1}+\frac{x}{n_2}=\frac{1}{n} \tag{11}$$

这证明了，只要知道圆周的$\frac{1}{n_1}$和$\frac{1}{n_2}$就可以求得圆周的$\frac{1}{n}$.

反之，若用规尺可以n等分圆周，且$n_1n_2=n \Longrightarrow \frac{1}{n_1n_2}=\frac{1}{n} \Longrightarrow \frac{1}{n_1}=n_2\frac{1}{n}$，$\frac{1}{n_2}=n_1\frac{1}{n}$. 即重复度量$n_2$次（$n_1$次）$\frac{1}{n}$圆周，就得到$\frac{1}{n_1}\left(\frac{1}{n_2}\right)$圆周的长度。

因为$x^n-1=0$的n个根：$x_k=\cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n}$（$k=0, 1, \cdots, n-1$），当$(k, n)=d$时，$x_k^{\frac{n}{d}}-1=0$，$s<\frac{n}{d}$时$x_k^s-1\neq0$。特别$d=1$时，$x_k^n-1=0$，而$t<n$时$x_k^t-1\neq0$，这样的$x_k$叫做n次单位质根或n次本原单位根。显然n次单位质根共有$\varphi(n)$个。割圆问题的实质就是n次单位质根的可作图问题，或者$n=p_1^{\alpha_1}\cdots p_t^{\alpha_t}$，转化为一切$p_i^{\alpha_i}$（$i=1, \cdots, t$）次的单位质根可作图。下面给出n等分圆周的割圆方程

$$\Phi_n(x)=\prod_{i=1}^{\varphi(n)}(x-\xi_i)=0$$

其中ξ_i为n次单位质根。$\Phi_n(x)$可由x^n-1中陆续除去x^d-1中的因式($d|n$, $0<d<n$)而得到，所以

$$\Phi_{p^\alpha}(x)=\frac{x^{p^\alpha}-1}{x^{p^{\alpha-1}}-1}=x^{p^{\alpha-1}(p-1)}+x^{p^{\alpha-1}(p-2)}+\cdots+1=0$$

是$n_1=p^\alpha$等分圆周的割圆方程。事实上，$x^{p^\alpha}-1=0$的一切非质根都是$x^{p^{\alpha-1}}-1$的根。

引理 2 $\Phi_{p^\alpha}(x)$在有理数域Δ内是既约的。

证明 令$x=z+1$，则

$$f(z)=\Phi_{p^\alpha}(z+1)=\frac{(z+1)^{p^\alpha}-1}{(z+1)^{p^{\alpha-1}}-1}$$

$$=\frac{z^{p^\alpha}-1+C_{p^\alpha}^1z^{p^\alpha}-2+\cdots+C_{p^\alpha}^1}{z^{p^\alpha}-1+C_{p^{\alpha-1}}^1z^{p^{\alpha-1}}-2+\cdots+C_{p^{\alpha-1}}^1} \tag{12}$$

(12)右边的商（是一个整式）除第一项（最高次项）外各项的系数都是p的倍数，且$z=0$时，(12)的常数项

$$f(0)=\frac{C^{1}_{p^{\alpha}}}{C^{1}_{p^{\alpha-1}}}=\frac{p^{\alpha}}{p^{\alpha-1}}=p\Longrightarrow p^{2}+f(0)$$

按爱氏判别法可知(12)在△内是既约的。

定理8的证明 设$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_t^{\alpha_t}$($p_1$，$p_2$，…，$p_t$是不同的素数）由引理1知道，可用规尺n等分圆周的充要条件是：能用规尺$p_i^{\alpha_i}(i=1,2,\cdots,t)$等分圆周。故只需证明$n=p^{\alpha}$的特殊情形就够了。

现在先求$\Phi_{p^{\alpha}}(x)$的正规域，由引理2知道$\Phi_{p^{\alpha}}(x)$在△上是既约的。今把$\Phi_{p^{\alpha}}(x)$的任一个根ξ添加于△，容易证明△(ξ)就是$\Phi_{p^{\alpha}}(x)$的正规域。事实上，因为$\Phi_{p^{\alpha}}(x)$的每一个根都是n次单位质根，它们都是单位质根ξ的乘幂（可参考高等代数二项方程一节，或者读者直接用单位根的三角表示式或指数表示式来证明），故都属于△(ξ)。

又因$\partial\Phi_{p^{\alpha}}(x)=p^{\alpha-1}(p-1)$，所以

$$(\triangle(\xi):\triangle)=p^{\alpha-1}(p-1)$$

由定理7知道，$\Phi_{p^{\alpha}}(x)$能还原成一串次数不高于二的方程的充要条件是：

$$(\triangle(\xi):\triangle)=p^{\alpha-1}(p-1)=2^{m}\Longrightarrow\begin{cases}(\text{i})\ p=2\\(\text{ii})\ \alpha=1\text{且}p=2^{k}+1\end{cases}$$

定理得证。

从这个定理知道，默森尼数M_p为素数时，M_p边的正多边形可以用规尺作图。

第八章　数论函数和素数分布

前几章我们已个别地提出了在数论中常用的若干函数，如，$[x]$，$\{x\}$，欧拉函数，勒让得符号，雅可比符号和特征函数等。这些函数都是数论函数。所谓数论函数一般是指在整数或正整数（本章整数都指有理整数）上有确定的值的函数。本章将进一步讨论几种数论函数，并简单地讨论素数在自然数列中的分布情况。本章的R是表示一切整数的集合，N表示一切正整数的集合．

第一节　可乘函数和莫比乌斯反转公式

定义8·1　若 $f(x)$是在一切正整数 a 上都有定义的函数，并且它具有下列二性质：

1°　有一个正整数 a，使得函数值 $f(a)\neq 0$；

2°　对于任何两个互素的正整数 a_1，a_2，都有

$$f(a_1 a_2)=f(a_1)f(a_2) \tag{1}$$

则称 $f(x)$为可乘函数（multiplicative function）．

如，前诸章所介绍的欧拉函数，勒让得符号，雅可比符号和特征函数等都是可乘函数．

例8·1　(i)　任给 $a\in N$，定义函数

$$\Delta(a)=\begin{cases}1，若 a=1，\\0，若 a\neq 1.\end{cases}$$

则$\Delta(a)$是一个可乘函数．

(ii)　若 λ 是任一给定的复数，对于任一 $a\in N$，定义

$$E_\lambda(a)=a^\lambda$$

则$E_\lambda(a)$是可乘函数。

(iii) 莫比乌斯（Möbius）函数：对于任一$a\in N$，定义

$$\mu(a)=\begin{cases}1，若 a=1; \\ (-1)^r，若 a 是 r 个不同素数之积; \\ 0，若 a 被一个素数的平方所整除.\end{cases}$$

则$\mu(a)$是一个可乘函数。

证明 由$\mu(a)$的定义知道，它满足定义8·1的条件1°。任给a_1，$a_2\in N$，$(a_1, a_2)=1$，若$a_1=1$（或$a_2=1$），或者存在某素数p使得$p^2|a_1$（或$p^2|a_2$），则(1)显然成立；若$a_1=p_1p_2\cdots p_r$，$a_2=q_1q_2$，q_s，其中p_1，p_2，…，p_r是两两互不相同的素数，q_1，q_2，…，q_s亦是两两互不相同的素数。由于$(a_1, a_2)=1$，故$p_i\neq q_j$($i=1$，…，r；$j=1$，…，s)。因此由定义

$$\mu(a_1a_2)=(-1)^{r+s}=(-1)^s(-1)^r=\mu(a_1)\mu(a_2)$$

所以$\mu(a)$是一个可乘函数。

容易算出：$\mu(1)=1$，$\mu(2)=-1$，$\mu(3)=-1$，$\mu(4)=0$，…，$\mu(20)=0$，$\mu(21)=1$，$\mu(22)=1$，$\mu(23)=-1$，$\mu(24)=0$…，

例8·2 令$r(a)$表示不定方程

$$a=x^2+y^2，a\in N$$

的整数解的个数，则$r(a)$不是可乘函数，因为$r(2)=4$，$r(5)=8$但$r(10)=8$。

例8·3 令$\pi(x)$表示不大于x的素数的个数，则$\pi(x)$不是可乘函数。因为$\pi(2)=1$，$\pi(3)=2$，但$\pi(6)=3$。

可乘函数有下列性质：

1° 若 $f(x)$ 是可乘函数，则 $f(1)=1$。

证明 由定义8·1，存在 $a\in N$ 使得 $f(a)\neq 0$，又 $f(a)=f(1)f(a)$，故 $f(1)=1$。

2° 若 $f_1(x)$，$f_2(x)$ 是两个可乘函数，则函数 $f(x)=f_1(x)f_2(x)$ 亦是可乘函数。

证明 因为 $f(1)=f_1(1)f_2(1)=1\cdot 1=1$，故 $f(x)$ 具有定义8·1的性质1°；任给 a_1，$a_2\in N$，$(a_1, a_2)=1$，则由定义8·1的2°，得

$$\begin{aligned} f(a_1a_2) &= f_1(a_1a_2)f_2(a_1a_2) \\ &= f_1(a_1)f_1(a_2)\cdot f_2(a_1)f_2(a_2) \\ &= [f_1(a_1)f_2(a_1)][f_1(a_2)f_2(a_2)] \\ &= f(a_1)\cdot f(a_2). \end{aligned}$$

即满足定义8·1的2°。所以 $f(x)$ 是可乘函数。

3° 若 $f(x)$ 是可乘函数，而正整数 a 的标准分解式是 $a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$，则

$$\sum_{d|a}f(d)=\prod_{i=1}^{k}\left(1+f(p_i)+f(p_i^2)+\cdots+f(p_i^{\alpha_i})\right) \quad (2)$$

其中 $\sum\limits_{d|a}$ 表示展布在 a 的一切正因数上的和式。

证明 由定理1·18系2知道，a 的任一正因数是：

$d=p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta_k}$，$\beta_i=0$，1，2，…，$\alpha_i$ $(i=1, 2, \cdots, k)$。

$$\begin{aligned} \therefore \sum_{d|a}f(d) &= \sum_{\beta_1=0}^{\alpha_1}\sum_{\beta_2=0}^{\alpha_2}\cdots\sum_{\beta_k=0}^{\alpha_k}f(p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta_k}) \\ &= \sum_{\beta_1=0}^{\alpha_1}\sum_{\beta_2=0}^{\alpha_2}\cdots\sum_{\beta_k=0}^{\alpha_k}f(p_1^{\beta_1})f(p_2^{\beta_2})\cdots f(p_k^{\beta_k}) \end{aligned}$$

$$=\prod_{i=1}^{k}(f(p_i^0)+f(p_i)+\cdots+f(p_i^{\alpha_i}))$$

而 $f(p_i^0)=f(1)=1$，故得(2)。

由例8·1(ii)并在性质3°中取 $f(d)=d^{\lambda}$，即得

4° 若 $a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ 是 a 的标准分解式，则

$$\sigma_\lambda(a)=\sum_{d|a}d^{\lambda}=\prod_{i=1}^{k}(1+p_i^{\lambda}+p_i^{2\lambda}+\cdots+p_i^{\alpha_i\lambda})$$

特别地，若以 $\sigma_1(a)=\sigma(a)$ 表示 a 的一切正因数的和，则

$$\sigma(a)=\prod_{i=1}^{k}(1+p_i+p_i^2+\cdots+p_i^{\alpha_i})=\prod_{i=1}^{k}\frac{p_i^{\alpha_i+1}-1}{p_i-1}$$

若以 $\tau(a)$ 表示 a 的正因数的个数，则

$$\tau(a)=(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_k+1) \qquad (3)$$

这时，$\tau(a)$ 叫做除数函数（divisor function）。由(3)容易证明 $\tau(a)$ 是一个可乘函数。

由性质2°，3°及例8·1(iii)，得

5° 若 $f(x)$ 是一个可乘函数，a 的标准分解式是

$$a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k},$$

则

$$\sum_{d|a}\mu(d)f(d)=(1-f(p_1))(1-f(p_2))\cdots(1-f(p_k)) \qquad (4)$$

证明 由性质2°知 $\mu(x)f(x)$ 是可乘函数，由性质3°，即得

$$\sum_{d|a}\mu(d)f(d)=\prod_{i=1}^{k}[1+\mu(p_i)f(p_i)+\mu(p_i^2)f(p_i^2)+$$

$$\cdots+\mu(p_i^{\alpha_i})f(p_i^{\alpha_i})]$$

因为 $\mu(p_i^2)=\cdots=\mu(p_i^{\alpha_i})=0$，$\mu(p_i)=-1(i=1,2,\cdots,k)$，故得(4)。

6° 若 $a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ 是 a 的标准分解式，则

$$\sum_{d\mid a}\mu(d)=\begin{cases}0, & 若\ a>1\\ 1, & 若\ a=1\end{cases} \tag{5}$$

$$\sum_{d\mid a}\frac{\mu(d)}{d}=\begin{cases}(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_k}), & 若\ a>1;\\ 1, & 若\ a=1.\end{cases} \tag{6}$$

证明 由莫比乌斯函数的定义及性质4°，立即得到，当 $a=1$ 时

$$\sum_{d\mid 1}\mu(d)=1,\quad \sum_{d\mid 1}\frac{\mu(d)}{d}=1;$$

$a>1$ 时，

$$\sum_{d\mid a}\mu(d)=(1+\mu(p_1))(1+\mu(p_2))\cdots(1+\mu(p_k))$$
$$=0$$

$$\sum_{d\mid a}\frac{\mu(d)}{d}=(1+\frac{\mu(p_1)}{p_1})(1+\frac{\mu(p_2)}{p_2})\cdots(1+\frac{\mu(p_k)}{p_k})$$
$$=(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_k})$$

定理8·1 任给 $\delta_1, \delta_2, \cdots, \delta_n\in N$，$f(\delta_1)$，$f(\delta_2)$，$\cdots$，$f(\delta_n)$ 是任意给定的 n 个复数。

$$s'=\sum_{\delta_i=1}f(\delta_i),\quad s_d=\sum_{d\mid\delta_i}f(\delta_i)$$

其中 $\sum\limits_{\delta_i=1}$ 表示展布在等于 1 的一切 δ_i 上的和式，$\sum\limits_{d\mid\delta_i}$ 表示对

于给定的 d，展布在 d 的倍数的一切 δ_i 上的和式，则

$$S' = \sum_{k=1}^{r} \mu(d_k) S_{d_k} \tag{7}$$

其中 d_1，d_2，…，d_r 是至少能整除一个 δ_i 的一切正整数。

证明 由(5)得

$$S' = f(\delta_1)\sum_{d|\delta_1}\mu(d) + f(\delta_2)\sum_{d|\delta_2}\mu(d) + \cdots$$

$$+ f(\delta_n)\sum_{d|\delta_n}\mu(d) \tag{8}$$

由于 d_k 至少整除一个 δ_i，因而(8)的右端有 $f(\delta_i)\cdot\mu(d_k)$ 项出现，把一切这样的项取出并相加，得

$$\mu(d_k)\sum_{d_k|\delta_i} f(\delta_i) = \mu(d_k) S_{d_k}.$$

由于 d_1，d_2，…，d_r 是至少能整除一个 δ_i 的一切正整数，故 $\mu(d_1)S_{d_1}$，$\mu(d_2)S_{d_2}$，…，$\mu(d_r)S_{d_r}$ 刚好包含着(8)的右端所出现的一切项，故(7)成立。

这是一条十分有用的定理，我们将应用这个定理，重新证明定理3·6，借以帮助读者更好地掌握它。

7° 对于任给的 $a \in N$，$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$，欧拉函数

$$\varphi(a) = a\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)$$

证明 令 $\delta_x = (x, a)$，$f(\delta_x) = 1 (x = 0, 1, \cdots, a-1)$，则由欧拉函数的定义及定理8·1中 S' 的定义知

$$S' = \sum_{\delta_x = 1} f(\delta_x) = \varphi(a)$$

而 S_d 是满足条件 $d|(x, a)$ 的 x 的个数，若 d 至少能整除一个 δ_x，则 $d|a$，而 S_d 是0，1，…，$a-1$ 中能被 d 整除的数

的个数，即

$$S_d=\left[\frac{a}{d}\right]=\frac{a}{d}\text{（因为}d\mid a\text{）。}$$

反之，对 a 的每一个正因数 d ，一定存在一个 δ_x 能被 d 整除，故由定理8·1知

$$\varphi(a)=\sum_{d\mid a}\mu(d)\frac{a}{d}=a\sum_{d\mid a}\frac{\mu(d)}{d}$$

从而由（6）得

$$\varphi(a)=a\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)\tag{9}$$

8° 若有N件事，其中具有性质α的有N_α件，具有性质β的有N_β件，兼有性质α和β的有$N_{\alpha\beta}$件，…，兼有性质α，β和γ的有$N_{\alpha\beta\gamma}$件，…等等。则都不具性质 α，β，γ，…的事物的件数是

$$N-N_\alpha-N_\beta-\cdots+N_{\alpha\beta}+\cdots-N_{\alpha\beta\gamma}-\cdots\tag{10}$$

证明 若一事物Q刚好具有 k 个性质α，β，…γ，则 Q 在和式(10)中出现的情况是：若 k≥1 ，则 Q在具有一个性质的事物N_α，N_β，…N_γ，…中出现$C_k^1=k$次；具有两个性质的事物$N_{\alpha\beta}$，$N_{\alpha\gamma}$，… 中 出 现 $C_k^2=\frac{k(k-1)}{2!}$ 次；在$N_{\alpha\beta\gamma}$，…中出现$C_k^3=\frac{k(k-1)(k-2)}{3!}$次，…，等等。所以若 k≥1时，事物Q在(10)中出现的次数是：

$$1-k+\frac{k(k-1)}{2!}-\frac{k(k-1)(k-2)}{3!}+\cdots$$
$$+(-1)^k\frac{k!}{k!}=(1-1)^k=0$$

另一种情况，若 k＝0，则每一个不具备任何性 质 的 事

物在(10)中出现一次。所以(10)是N个事物中不具备任一性质的事物的总数。

9° 若$\{a, b, c, \cdots\}$是两两互素的正整数的集合，则小于或等于n且不被a，b，…所整除的整数的数目是

$$[n]-\sum\left[\frac{n}{a}\right]+\sum\left[\frac{n}{ab}\right]-\cdots$$

这个性质是性质8°中用a，b，…代表不同的性质直接得到的结果。

若在性质9°中，取n为正整数，a，b，…为n的不同素因数p_1，p_2，…，p_k，就得到

10° 若$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$，则

$$\begin{aligned}\varphi(n)&=n-\sum_{i=1}^{k}\left[\frac{n}{p_i}\right]+\sum_{i\neq j}\left[\frac{n}{p_ip_j}\right]-\cdots\\&\quad+(-1)^k\left[\frac{n}{p_1p_2\cdots p_k}\right]\\&=n-\sum_{i=1}^{k}\frac{n}{p_i}+\sum_{i\neq j}\frac{n}{p_ip_j}-\cdots+(-1)^k\frac{n}{p_1p_2\cdots p_k}\\&=n\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)\end{aligned}\tag{11}$$

11° $$n=\sum_{d\mid n}\varphi(d)\tag{12}$$

证明 对于n个正分数

$$\frac{h}{n}(1\leqslant h\leqslant n)\tag{13}$$

中的每一个分数都有$\frac{h}{n}=\frac{a}{d}$，其中$d\mid n$，$(a, d)=1$，这里的

$\frac{a}{d}$是一个既约分数，$1\leqslant a\leqslant d$. 这样的 a 和 d 是由 h 和 n 所唯一确定的. 反之，分数$\frac{a}{d}$亦唯一确定（13）中的一个分数$\frac{h}{n}$. 也就是说，对任一函数 $F(x)$，我们有

$$\sum_{1\leqslant h\leqslant n} F\left(\frac{h}{n}\right)=\sum_{d\mid n}\ \sum_{\substack{1\leqslant a\leqslant d\\(a,d)=1}} F\left(\frac{a}{d}\right) \tag{14}$$

对于给定的特殊的 d，满足$(a,\ d)=1$且$1\leqslant a\leqslant d$的 a 刚好$\varphi(d)$个值，即在(14)右边的和式中，出现以 d 为分母的分数刚好有$\varphi(d)$个. 取$F(x)=1$，则(14)的左边$=n$，右边$=\sum\limits_{d\mid n}\varphi(d)$，因而

$$n=\sum_{d\mid n}\varphi(d)$$

这是定理3·6系2的结论。

12° 若 $f(n)$是可乘函数，则

$$g(n)=\sum_{d\mid n} f(n)$$

亦为可乘函数。

证明 若$(n,\ n')=1$，$d\mid n$ 且 $d'\mid n'$，则$(d,\ d')=1$ 并且 $c=dd'$ 跑过 nn' 的全体因数，所以

$$g(nn')=\sum_{c\mid nn'} f(c)=\sum_{d\mid n,d'\mid n'} f(dd')$$

$$=\left[\sum_{d\mid n} f(d)\right]\left[\sum_{d'\mid n'} f(d')\right]$$

$$=g(n)g(n')$$

这就适合了定义8·1的条件2°。

由于 $f(x)$是可乘函数，由性质1°知 $f(1)=1$，$g(1)=\sum_{d|1} f(d)=1$，所以适合定义8·1的条件1°，故 $g(n)$亦为可乘函数。

由性质6°与7°，即得

13° $\varphi(n)=n\sum_{d|n}\frac{\mu(d)}{d}=\sum_{d|n}\frac{n}{d}\mu(d)$

$$=\sum_{d|n}d\,\mu\left(\frac{n}{d}\right)\sum_{dd'=n}d'\mu(d) \qquad (15)$$

例如，$n=120=2^3\times3\times5$，$\varphi(120)=32$，而 $\sum_{d|n}\frac{n}{d}\mu(d)$

$$=120-\frac{120}{2}-\frac{120}{3}-\frac{120}{5}+\frac{120}{6}+\frac{120}{10}+\frac{120}{15}-\frac{120}{30}=32,$$

$$\sum_{dd'=n}d'\mu(d)=120\mu(1)+60\mu(2)+40\mu(3)+24\mu(5)$$

$$+20\mu(6)+12\mu(10)+8\mu(15)+4\mu(30)=32.$$

14° 若 $n>1$，且 n 含有 k 个不同的素因数，则

$$\sum_{d|n}\left|\mu(d)\right|=2^k \qquad (16)$$

证明 若 $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$，则

$$\sum_{d|n}\left|\mu(d)\right|=(1+|\mu(p_1)|)(1+|\mu(p_2)|)\cdots$$

$$(1+|\mu(p_k)|)=(1+1)^k=2^k$$

若用 $\mu(d)$代替性质12°中的 $f(d)$，并由(5)得到

15° $g(n)=\sum_{d|n}\mu(d)$是一个可乘函数，并且

$$g(n)=\begin{cases}1, & 若\ n=1\\ 0, & 若 n>1\end{cases}$$

下面介绍莫比乌斯反转公式（Möbius inversion formula)。

定理8·2 若 $f(n)$，$g(n)$是任二可乘函数，且

$$g(n)=\sum_{d\mid n}f(d)$$

则

$$f(n)=\sum_{d\mid n}\mu\left(\frac{n}{d}\right)g(d)=\sum_{d\mid n}\mu(d)g\left(\frac{n}{d}\right) \tag{17}$$

证明 设$\frac{n}{d}=d'$，即 $dd'=n$，则

$$\sum_{d\mid n}\mu(d)g(d')=\sum_{d\mid n}\mu(d)\sum_{c\mid d'}f(c)=\sum_{cd\mid n}\mu(d)f(c)$$

$$=\sum_{c\mid n}f(c)\sum_{d\mid \frac{n}{c}}\mu(d)$$

由性质6°知，其内部之和当 $c=n$ 时为1，$c<n$ 时为0，故上式右边等于 $f(n)$。

这个定理的逆定理亦成立。

定理8·3 若 $g(n)$，$f(n)$是两个可乘函数，且

$$f(n)=\sum_{d\mid n}\mu\left(\frac{n}{d}\right)g(d)$$

则

$$g(n)=\sum_{d\mid n}f(d) \tag{18}$$

证明 其证法与定理8·2相似，我们有

$$\sum_{d|n} f(d) = \sum_{d|n} f\left(\frac{n}{d}\right) = \sum_{d|n} \sum_{c|\frac{n}{d}} \mu\left(\frac{n}{cd}\right) g(c)$$

$$= \sum_{cd|n} \mu\left(\frac{n}{cd}\right) g(c) = \sum_{c|n} g(c) \sum_{c|\frac{n}{c}} \mu\left(\frac{n}{cd}\right)$$

$$= g(n)$$

定义8·2 若

$$g(n) = \sum_{d|n} f(d) = \sum_{d|n} f\left(\frac{n}{d}\right)$$

则 $g(n)$叫做 $f(n)$的莫比乌斯变换（Möbius′ transformation）而 $f(n)$叫做 $g(n)$的莫比乌斯逆变换（Möbius′ inverse transformation）。

由定理8·2知道，可乘函数的莫比乌斯变换及莫比乌斯逆变换也是可乘函数。

如果我们取 $g(n)=n$，那末由定理8·3及(15)，得到 $\varphi(n)=f(n)$；并从(18)得到性质11°。

我们假设 $d|p-1$且 $c|d$，用函数 $\chi(c)$来表示同余式 $x^d \equiv 1 \pmod p$的根中属于方次数 c 的根的个数，因为这个同余式共有 d 个根，所以

$$\sum_{c|d} \chi(c) = d \tag{19}$$

在定理8·2中取 $g(n)=n$，从上式得

16° $$\chi(d) = \sum_{c|d} \mu(c)\frac{d}{c} = \varphi(d) \tag{20}$$

下面讨论包括 $\mu(n)$在内的更一般的反转公式

定理8·4 若对全体正数 x

$$G(x)=\sum_{n=1}^{[x]}F\left(\frac{x}{n}\right) \tag{21}$$

其中当$[x]=0$时，右边空和式看作0，则

$$F(x)=\sum_{n=1}^{[x]}\mu(n)G\left(\frac{x}{n}\right) \tag{22}$$

证明 由(21)及性质12°，得

$$\sum_{n=1}^{[x]}\mu(n)G\left(\frac{x}{n}\right)=\sum_{n=1}^{[x]}\left\{\mu(n)\sum_{m=1}^{[x/n]}F\left(\frac{x}{mn}\right)\right\}$$

$$=\sum_{1\leqslant k\leqslant[x]}\left\{F\left(\frac{x}{k}\right)\sum_{n\mid k}\mu(n)\right\}$$

$$=F(x)$$

其中，若$mn=k$，则$n\mid k$，并且k遍取数目1，2，…，$[x]$。事实上，

$$\sum_{n=1}^{[x]}\left\{\mu(n)\sum_{m=1}^{[x/n]}F\left(\frac{x}{mn}\right)\right\}=\mu(1)\sum_{m=1}^{[x]}F\left(\frac{x}{m}\right)$$

$$+\mu(2)\sum_{m=1}^{[x/2]}F\left(\frac{x}{2m}\right)+\cdots+\mu([x])F\left(\frac{x}{[x]}\right)$$

而

$$\sum_{1\leqslant k\leqslant[x]}\left\{F\left(\frac{x}{k}\right)\sum_{n\mid k}\mu(n)\right\}=F\left(\frac{x}{1}\right)\mu(1)$$

$$+F\left(\frac{x}{2}\right)\left\{\mu(1)+\mu(2)\right\}+F\left(\frac{x}{3}\right)\left\{\mu(1)+\mu(3)\right\}$$

$$+F\left(\frac{x}{4}\right)\left\{\mu(1)+\mu(2)\right\}+\cdots$$

$$+F\left(\frac{x}{[x]}\right)\sum_{n\mid[x]}\mu(n)$$

整理后，显然上二式的右边相等，并且由(5)知道上式右边除第一项 = F(x) 外，其余诸项都等于0，故上式右边等于F(x)。

类似于定理8·4容易证明它的逆定理亦成立(留给读者作练习)．即有

定理8·5 若对于全体正数 x，都有

$$F(x)=\sum_{n=1}^{[x]}\mu(n)G\left(\frac{x}{n}\right)$$

则

$$G(x)=\sum_{n=1}^{[x]}F\left(\frac{x}{n}\right)$$

定理8·4，8·5的反转公式，实际上包含于

定理8·6 $g(x)=\sum_{m=1}^{\infty}f(mx)\Longleftrightarrow f(x)$

$$=\sum_{m=1}^{\infty}\mu(n)g(nx).$$

证明 令 $\tau(k)$表示 k 的正因数的个数(除数函数)．则

$$\sum_{m,n}f(mnx)=\sum_{k}\tau(k)f(kx)\quad(k=mn)$$

这里 $n|k$，$k=1, 2, 3, \cdots$。

若 $g(x)=\sum_{m=1}^{\infty}f(mx)$，则由(5)得

$$\sum_{n=1}^{\infty}\mu(n)g(nx)=\sum_{n=1}^{\infty}\left\{\mu(n)\sum_{m=1}^{\infty}f(mnx)\right\}$$

$$=\sum_{n=1}^{\infty}\left\{\sum_{m=1}^{\infty}f(mnx)\right\}\mu(n)$$

$$=\sum_{n|k}\left\{\sum_{k=1}^{\infty}\tau(k)f(kx)\right\}\mu(n)=f(x).$$

反之，可类似地证明。

第二节　函数$e(\tau)$，$S(m, n)$，$Cg(m)$，$S(u, v, n)$和$r(n)$

一、三角和（trigonometric sum）.

对任一有理数τ三角和$e(\tau)$定义为：

$$e(\tau)=e^{2\pi i\tau},\quad \tau=\frac{m}{n},\ m,\ n\text{是整数},\ n>0 \tag{23}$$

当$m\equiv m'(\mathrm{mod}\ n)$时，显然有

$$e\left(\frac{m}{n}\right)=e\left(\frac{m'}{n}\right)$$

这是三角和的重要的算术性质。

二、高斯和（Gauss' Sum）.

高斯和$S(m, n)$指的是

$$S(m, n)=\sum_{h=0}^{n-1}e^{2\pi ih^2\frac{m}{n}}=\sum_{h=0}^{n-1}e\left(\frac{h^2m}{n}\right) \tag{24}$$

由于对于任一整数r，我们有

$$e\left(\frac{(h+rn)^2m}{n}\right)=e\left(\frac{h^2m}{n}\right)$$

即，当$h_1\equiv h_2(\mathrm{mod}\ n)$时，$e\left(\frac{h_1{}^2m}{n}\right)=e\left(\frac{h_2^2m}{n}\right)$。故高斯和又可写作

$$S(m, n)=\sum_{h(n)} e\left(\frac{h^2 m}{n}\right) \tag{24'}$$

这里 h(n)是过模 n 的完全剩余系，在不会发生混淆的情 况下，用 h 代表 h(n)。

16° 若$(n, n')=1$，则

$$S(m, nn')=S(mn', n)S(mn, n')$$

证明 若 h，h′ 分别为过模 n，n′ 的完全剩余 系，由定理3·5系 1 知道

$$H=hn'+h'n$$

为过模 nn′的完全剩余系，而

$$mH^2=m(hn'+h'n)^2\equiv mh^2n'^2+mh'^2n^2 \pmod{nn'}$$

$$\therefore\quad S(mn', n)S'(mn, n')$$

$$=\left\{\sum_h e\left(\frac{h^2mn'}{n}\right)\right\}\left\{\sum_{h'} e\left(\frac{h'^2mn}{n'}\right)\right\}$$

$$=\sum_{h,h'} e\left(\frac{h^2mn'}{n}+\frac{h'^2mn}{n'}\right)$$

$$=\sum_{h,h'} e\left(\frac{m(h^2n'^2+h'^2n^2)}{nn'}\right)$$

$$=\sum_H e\left(\frac{mH^2}{nn'}\right)=S(m, nn')$$

这条性质是高斯和的一条可乘性质，它在研究平方剩余的理论中是很有用的。

三、李曼留振和（Ramanujan's Sum)。

李曼留振和指的是如下的函数：

$$Cq(m)=\sum_{h^*(q)} e\left(\frac{hm}{q}\right) \tag{25}$$

其中 $h^*(q)$是过模 q 的互素剩余系，在不会引起混乱的情况下，用 h 代替 $h^*(q)$。

我们称 ρ 为 q次本原单位根，如果存在正整数 q，使得 $\rho^q=1$，且当 $0<r<q$ 时，$\rho^r\neq 1$。

17° 在 q 次单位根中，若 ρ 是其中任一 r 次本原单位根，则 r 必整除 q。

证明 若 ρ 是 $x^q=1$的一个解，并且 $\rho^r=1$，$0<r<q$，而当$0<s<r$ 时 $\rho^s\neq 1$。因为 $q=kr+s$，$0\leqslant s<r$，所以

$$\rho^q=\rho^{kr}\cdot\rho^s=\rho^s\Longrightarrow 1=\rho^s\Longrightarrow s=0\Longrightarrow r\mid q.$$

18° q 次单位根是形如

$$e\left(\frac{h}{q}\right)\quad (h=0,\ 1,\ \cdots,\ q-1)$$

的数，并且当且仅当$(h,\ q)=1$ $e\left(\frac{h}{q}\right)$是 q 次本原单位根

证明 $\left[e\left(\frac{h}{q}\right)\right]^q=e^{2\pi ih}=1$

$$\because\qquad q\mid hr\Longleftrightarrow\left[e\left(\frac{h}{q}\right)\right]^r=e\left(\frac{hr}{q}\right)=1$$

$$\therefore\qquad (q,\ h)=1\Longleftrightarrow\left[e\left(\frac{h}{q}\right)\right]^r\neq 1\quad (0<r<q)$$

有了性质18°，李曼留振和可改写为

$$C_q(m)=\sum_{\rho}\rho^m$$

其中 ρ 是过 q 次的一切本原单位根。

$C_q(m)$具有如下的可乘性质：

19° 若$(q,\ q')=1$，则

$$C_{qq'}(m)=C_q(m)C_{q'}(m)$$

证明 由定理3·5系3，得

$$C_q(m)C_{q'}(m)=\sum_{h^*(q),h^*(q')} e\left(m\left(\frac{h}{q}+\frac{h'}{q'}\right)\right)$$

$$=\sum_{h,h'} e\left(\frac{m(hq'+h'q)}{qq'}\right)$$

$$=C_{qq'}(m)$$

在(25)中取 $q=n$，得

$$C_n(m)=\sum_{\substack{1\leqslant h\leqslant n\\(h,n)=1}} e\left(\frac{hm}{n}\right) \tag{25'}$$

我们可以把$C_n(m)$表示为 m 和 n 的公因数的和。

20° $$C_n(m)=\sum_{d|m,d|n}\mu\left(\frac{n}{d}\right)d \tag{26}$$

证明 如果我们取

$$g(n)=\sum_{1\leqslant h\leqslant n}F\left(\frac{h}{n}\right),\quad f(n)=\sum_{\substack{1\leqslant h\leqslant n\\(h,n)=1}}F\left(\frac{h}{n}\right)$$

那末(14)成为

$$g(n)=\sum_{d|n}f(d)$$

由定理8·2，我们有反转公式

$$f(n)=\sum_{d|n}\mu\left(\frac{n}{d}\right)g(d)$$

$$=\sum_{d|n}\left\{\mu\left(\frac{n}{d}\right)\sum_{1\leqslant a\leqslant d}F\left(\frac{a}{d}\right)\right\} \tag{27}$$

$$\therefore\quad \sum_{\substack{1\leqslant h\leqslant n\\(h,n)=1}}F\left(\frac{h}{n}\right)=\sum_{d|n}\left\{\mu\left(\frac{n}{d}\right)\sum_{1\leqslant a\leqslant d}F\left(\frac{a}{d}\right)\right\} \tag{28}$$

取$F(x)=e(mx)$，此时 $f(n)=C_n(m)$由(25′)，得

$$g(n)=\sum_{1\leqslant h\leqslant n} e\left(\frac{hm}{n}\right)=\begin{cases} n, & 当\ n\mid m\ 时 \\ 0, & 当\ n\nmid m\ 时 \end{cases}$$

因而

$$C_n(m)=f(n)=\sum_{d\mid m}\mu\left(\frac{n}{d}\right)g(d)=\sum_{d\mid n, d\mid m}\mu\left(\frac{n}{d}\right)d$$

这就证明了(26)成立。

若在(21)中取 $m=1$，则$C_n(1)=\mu(n)$，从而有

21° $$\mu(n)=\sum_{\substack{1\leqslant h\leqslant n\\(h,n)=1}} e\left(\frac{h}{n}\right)$$

四、克鲁斯特曼和(Kloosterman's sum)

克鲁斯特曼和是指如下的函数：

$$S(u, v, n)=\sum_{h} e\left(\frac{uh+v\bar{h}}{n}\right) \tag{29}$$

这里 h 为过 n 的互素剩余系，并且 $\bar{h}$是$h\bar{h}\equiv1(\bmod n)$的解，给定 h 之后，$\bar{h}$是唯一确定的。

克鲁斯特曼和有如下的可乘性质：

22° 若$(n, n')=1$，则

$$S(u, v, n)S(u, v', n')=S(u, V, nn')$$

其中$V=vn'^2+v'n^2$。

证明 若$h\bar{h}\equiv1(\bmod n)$，$h'\bar{h'}\equiv1(\bmod n')$，则

$$S(u, v, n)S(u, v', n')$$

$$=\sum_{h,h'} e\left(\frac{uh+v\bar{h}}{n}+\frac{uh'+v'\bar{h'}}{n'}\right)$$

$$=\sum_{h,h'} e\left(u\cdot\frac{hn'+h'n}{nn'}+\frac{v\bar{h}n'+v'\bar{h}'n}{nn'}\right)$$

$$=\sum_{h,h'} e\left(\frac{uH+K}{nn'}\right) \qquad (\alpha)$$

其中$H=hn'+h'n$，$K=v\bar{h}n'+v'\bar{h}'n$。由定理 3·5系 3 知道，H为过 nn' 的互素乘余系。因此，如果我们能证明：当$H\bar{H}\equiv 1 \pmod{nn'}$时，有

$$K\equiv V\bar{H} \pmod{nn'} \qquad (\beta)$$

那末(β)便成为

$$S(u, v, n)S(u, v', n')=\sum_{H} e\left(\frac{uH+V\bar{H}}{nn'}\right)$$

$$=S(u, V, nn')$$

下面将证明(β)。因为$(hn'+h'n, nn')=1$，故

$$(hn'+h'n)\bar{H}=H\bar{H}\equiv 1 \pmod{nn'}$$

有解$\bar{H}$，因而

$$hn'\bar{H}\equiv 1 \pmod{n} \Longrightarrow n'\bar{H}\equiv \bar{h} \pmod{n}$$

$$\Longrightarrow n'^2\bar{H}\equiv n'\bar{h} \pmod{nn'} \qquad (\gamma)$$

类似地，可得

$$n^2\bar{H}\equiv n\bar{h}' \pmod{nn'} \qquad (\delta)$$

由(γ)和(δ)我们便得到

$$V\bar{H}=(vn'^2+v'n^2)\bar{H}\equiv vn'\bar{h}+v'n\bar{h}'\equiv K \pmod{nn'}$$

从而就证明了(β)。

五　函数 $r(n)$

我们定义 $r(n)$为正整数 n 表成二个整数 A,B 的平方和

$$n = A^2 + B^2 \tag{30}$$

的数目，即满足(30)的整数对(A，B)的个数．如，$0 = 0^2 + 0^2$，$r(0) = 1$；$1 = (\pm 1)^2 + 0 = 0^2 + (\pm 1)^2$，$r(1) = 4$；$2 = (\pm 1)^2 + (\pm 1)^2$，$r(2) = 4$；$5 = (\pm 1)^2 + (\pm 2)^2 = (\pm 2)^2 + (\pm 1)^2$，$r(5) = 8$等等。

从第五章和第七章中知道，当 n 是$4n+1$形的素数时，$r(n) = 8$；n 是$4m+3$形的素数时，$r(n) = 0$

对于一切正整数 n，我们定义 $\chi(n)$如下：

$$\chi(n) = \begin{cases} 0, & \text{当 } 2 \mid n \text{ 时} \\ (-1)^{\frac{1}{2}(n-1)}, & \text{当} 2 \nmid n \text{ 时} \end{cases}$$

如此，对于 $n = 1, 2, 3, 4, 5, \cdots$时，$\chi(n) = 1, 0, -1, 0, 1$。即当 $n = 4m+1$时，$\chi(n) = 1$；当 $n = 4m+3$时，$\chi(n) = -1$；当 $n = 2m$时，$\chi(n) = 0$。于是当 n 和 n′ 都是奇数时，

$$\frac{1}{2}(nn' - 1) - \frac{1}{2}(n-1) - \frac{1}{2}(n'-1)$$

$$= \frac{1}{2}(n-1)(n'-1)$$

$$\equiv 0 \pmod 2$$

$$\therefore \quad (-1)^{\frac{1}{2}(nn'-1)}$$

$$= (-1)^{\frac{1}{2}(n'-1)} \cdot (-1)^{\frac{1}{2}(n-1)}$$

从而对一切正整数 n 和 n′，都有

23° $\chi(nn') = \chi(n)\chi(n')$

显然，若令

$$\delta(n) = \sum_{d \mid n} \chi(d) \tag{31}$$

则由 $\chi(n)$的定义，即得

$$\delta(x)=\tau_1(n)-\tau_3(n) \tag{32}$$

其中 $\tau_1(n)$和 $\tau_3(n)$分别是 n 的4m+1形和 4m+3形的因数的个数。

今设

$$n=2^\alpha, \quad N=2^\alpha\mu\upsilon=2^\alpha\prod p^r\prod q^s, \tag{33}$$

这里 p，q 分别是4m+1形和4m+3形的素数。若 n 没有因子 q（或p），则我们定义 $\upsilon=1$，$\mu=1$。
因而

$$\delta(n)=\delta(N)$$

N的一切因数是包含在下面乘积的各项中：

$$\prod(1+p+\cdots+p^r)\prod(1+q+\cdots+q^s) \tag{34}$$

偶数个4m+3形因数之积是4m+1形的因数，反之，奇数个 q 之积是4m+3形，而4m+1形因子与 4m+1 形因子之积，都是4m+1形。故 $\delta(N)$可由(34)中用 1 代 p，−1代 q而得到，即

$$\delta(N)=\prod(1+r)\prod\left(\frac{1+(-1)^s}{2}\right) \tag{35}$$

若有一个 s 是奇数时，即υ不是一个平方数时，则

$$\delta(n)=\delta(N)=0$$

若υ是一个数的平方时，则

$$\delta(n)=\delta(N)=\prod(1+r)=\tau(\mu).$$

我们有 $r(n)$的公式：

定理8·7 若 $n\geqslant1$，则

$$r(n)=4\delta(n) \tag{36}$$

系 把 n 表成(33)的形式时，若υ是一个数的平方，则

$$r(n)=4\delta(\mu)$$

若υ不是一个数的平方时，则

$$r(n)=0$$

这就证明了第五章第七节的结论：一个正整数 n 能表成两个整数的平方和的充要条件是：n 不含 $4m+3$ 形的素数的奇次因子，并且有解时，其解数是 $r(n)=4\delta(\mu)$

如，若 $n=7$，13×7，$4\times13\times7$ 时，(30)无解．而 $n=13$，$r(13)=4(1+1)=8$；$n=13\times37^2$，$r(13\times37^2)=4(1+1)(1+2)=24$；$n=13\times7\times11$，$r(13\times7\times11)=0$；$n=7^2\times11^2\times13^2$，$r(7^2\times11^2\times13^2)=4(1+2)=12$ 等等．

下面证明 $r(n)$ 的公式．由定理5·9的系知道，当 $p=4m+1$ 为素数时，存在二正整数 a 和 b，使得

$$p=a^2+b^2$$

于是可以把(33)改写为

$$n=\left\{(1+i)(1-i)\right\}^{\alpha}\prod\left\{(a+bi)(a-bi)\right\}^{r}\prod q^{s} \qquad (33)'$$

在第七章中已证明在不计 a，b 的顺序时，$p=a^2+b^2$ 的表示法是唯一的。因数 $1\pm i$，$a\pm bi$，q 在 $R[i]$ 里都是素数．若

$$n=A^2+B^2=(A+Bi)(A-Bi)$$

则

$$\begin{cases} A+Bi=i^{t}(1+i)^{\alpha_1}(1-i)^{\alpha_2}\prod\left\{(a+bi)^{r_1}\times(a-bi)^{r_2}\right\}\prod q^{s_1} \\ A-Bi=i^{-t}(1-i)^{\alpha_1}(1+i)^{\alpha_2}\prod\left\{(a-bi)^{\alpha_2}\times(a+bi)^{r_2}\right\}\prod q^{s_2} \end{cases} \qquad (37)$$

这里 $t=0$，1,2 或 3，$\alpha_1+\alpha_2=\alpha$，$r_1+r_2=r$，$s_1+s_2=s$，因为 q^{s_1}，q^{s_2} 是实数，所以 $s_1=s_2$，$s=2s_1$ 为偶数，即υ是一个整数的平方，否则 n 不能表为两个整数的平方和 .我们可设

$$\upsilon=\prod q^s=\prod q^{2s_1}=k^2$$

由于 $k|A$且 $k|B$，因此A，B的选择方法与因子 q 无关。而(37)的其他因子中的选择方法共有

$$4(\alpha+1)\prod(r+1) \tag{38}$$

种。但

$$\frac{1-i}{1+i}=-i,\ \frac{1+i}{1-i}=i$$

都是一个单位，因此改变积中的 α_1和α_2而不改变A和B（只是它的相伴数），除了变数 t 的选择之外，亦即积中的 $i^t(1+i)^{\alpha_1}(1-i)^{\alpha_2}$ 有且只有四种不同的选择方法（$t=0$，1，2，3）。例如，$\alpha=3$有

$$i^t(1+i)^0(1-i)^3=-2i^{t+1}(1-i)=-2i(1-i),$$
$$2(1-i),\ 2i(1-i)\text{或}-2(1-i);$$
$$i^t(1+i)(1-i)^2=2i^t(1-i)=2(1-i),\ 2i(1-i),$$
$$-2(1-i)\text{或}-2i(1-i);$$
$$i^t(1+i)^2(1-i)=2i^{t+1}(1-i)=2i(1-i),\ -2(1-i),$$
$$-2i(1-i)\text{或}2(1-i);$$
$$i^t(1+i)^3(1-i)^0=i^t(1+i)^2\frac{1+i}{1-i}(1-i)$$
$$=-2i^t(1-i)$$
$$=-2(1-i),\ -2i(1-i),2(1-i)$$

或$2i(1-i)$ 所以(37)左边有且只有

$$4\prod(r+1)=4\tau(\mu)$$

种的选择方法。即A，B共有$4\tau(\mu)$种不同的选择方法。如

$$1\cdot(A+Bi)=A+Bi;\qquad i(A+Bi)=-B+Ai;$$
$$i^2(A+Bi)=-A-Bi;\qquad i^3(A+Bi)=B-Ai.$$

及这四个数的共轭复数：$A-Bi$，$-B-Ai$，$-A+Bi$，$B+Ai$。任意改变t只不过把$A+Bi$或它的共轭数$A-Bi$换成它的相伴数。任意改变r_1和r_2也变化(37)的表示，但并不换成相伴数，故不能从t的改变来解析。因为

$$i^t(1+i)^{\alpha_1}(1-i)^{\alpha_2}\prod\left\{(a+bi)^{r_1}(a-bi)^{r_2}\right\}$$
$$=i\theta\, i^{t_1}(1+i)^{\alpha_1'}(1-i)^{\alpha_2'}\cdot$$
$$\cdot\prod\left\{(a+bi)^{r_1'}(a-bi)^{r_2'}\right\}$$

是不可能的。由于在R〔i〕中算术基本定理成立，故除非$r_1=r_1'$，$r_2=r_2'$*外上式不成立。所以A，B的值，或者说n的表示法共有$4\tau(\mu)$种，这就证明了定理8·7。

第三节　完全数

定义8·2　一个正整数n的一切正因数之和等于2n，即$\sigma(n)=2n$，则称n为完全数(perfect numbers)或称完美数。

例如，$1+2+3+6=2\times6$；$1+2+4+7+14+28=2\times28$所以6和28都是完全数。

古希腊毕达哥达斯学派已经提出，完全数就是一个数等于它的所有因数（除本身外的一切正因数）之和，如6，28与

* 当换r_1为r_2，r_2为r_1时，$A+Bi$变成它的共轭数$A-Bi$。

496便是完全数。并给出定义：数本身大于其因数之和者为盈数(excessive numbers 或 number of excess)；数本身小于其因数之和者为亏数(number of deficiency或 deficient numder)；如，12是盈数，14是亏数。若有两数彼此等于另一数因数之和，他们称这两数为亲和数(kindred numbers)，如，284和220是亲和数。实际上，若n为盈数则$\sigma(n)>2n$，亏数则$\sigma(n)<2n$；若m，n为亲和数，则$\sigma(m)-m=n$，$\sigma(n)-n=m$。

欧几里德《几何原本》第九篇第35题给出了：若几何级数

$$1+2+2^2+\cdots+2^{n-1}$$

之和是素数，则$(1+2+2^2+\cdots+2^{n-1})2^{n-1}=(2n^n-1)2^{n-1}$是完全数。这样的数后人把它叫做欧几里德数。从而得到前面四个完全数6，28，496，8128，也许还有第五个完全数。实际上，欧几里德给出了一切偶完全数的定理。

定理8·8 若$p=2^n-1$为素数，则

$$\frac{1}{2}p(p+1)=2^{n-1}(2^n-1)$$

是完全数，并且无其他偶完全数存在。

要证明这个定理需先证明

引理1 若$m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots,\ p_k^{\alpha_n}$，则

$$\sigma(m)=\frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdot\frac{p_2^{\alpha_2+1}-1}{p_2-1}\cdot\cdots\frac{p_k^{\alpha_n+1}-1}{p_k-1}$$

证明 由$\sigma(m)$的定义知

$$\sigma(m)=\sum_{d/m}d=(1+p_1+\cdots+p_1^{\alpha_1})(1+p_2+\cdots+p_2^{\alpha_2})$$

$$\cdots(1+p_k+\cdots+p_k^{\alpha_k})$$

$$=\frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdot\frac{p_2^{\alpha_2+1}-1}{p_2-1}\cdots\frac{p_k^{\alpha_k+1}-1}{p_k-1}$$

引理2　若$(m, n)=1$，则$\sigma(mn)=\sigma(m)\cdot\sigma(n)$。

证明　设 $m=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$，$n=q_1^{\beta_1}\cdots q_s^{\beta_s}$，则

$mn=p_1^{\alpha_1}\cdots p_k^{\alpha_k}\cdot q_1^{\beta_1}\cdots q_s^{\beta_s}$，$p_i$，$q_j$是均不相同的素数。

$$\therefore\quad \sigma(mn)=\frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdots\frac{p_k^{\alpha_k+1}-1}{p_k-1}\times\frac{q_1^{\beta_1+1}-1}{q_1-1}\cdots\frac{q_s^{\beta_s+1}-1}{q_s-1}=\sigma(m)\cdot\sigma(n).$$

定理8·8的证明：令$N=\frac{1}{2}p(p+1)=2^{n-1}(2^n-1)$，则由引理1得

$$\sigma(N)=\sigma(2^{n-1}p)=\frac{2^n-1}{2-1}\cdot\frac{p^2-1}{p-1}=(2^n-1)(p+1)=p(p+1)=2N.$$

所以N是完全数。

其次，若a是一个偶完全数，令

$$a=2^{n-1}u,\ n>1,\ 2\nmid u$$

由$\sigma(a)=2a=2^n u$及引理2，得

$$\sigma(a)=\sigma(2^{n-1})\sigma(u)=2^n u$$

从而得

$$(2^n-1)\sigma(u)=2^n u$$

$$\therefore\quad \sigma(u)=\frac{2^n u}{2^n-1}=u+\frac{u}{2^n-1},$$

但是 u 及$\frac{u}{2^n-1}$都是 u 的因数，而 $\sigma(u)$ 是 u 的一切因数之和，故 u 有且只有两个因数 u 和$\frac{u}{2^n-1}$，即 u 是素数且 $u=2^n-1$，也就是

$$a=2^{n-1}(2^n-1),\quad p=2^n-1\text{为素数。}$$

是否有奇完全数存在是数论中的著名难题，至今仍未解决。而求偶完全数的问题与求 $p=2^n-1$ 为素数的问题一致。由定理1·17知道，要 a^n-1 为素数，必须 $a=2$，$n=q$ 为素数，所以关于偶完全数的存在性、存在的数量以及求法的问题与求默森尼数（指的是 M_p 为素数）一致。第一章第五节已附有到1985年 9 月为止已发现的29个默森尼数 $M_p=2^p-1$，故已发现29个相应的完全数 $N_p=2^{p-1}(2^p-1)$，其中 $p=2$，3，5，7，…，23209，44497，86243，216091（如第一章第五节中所列的），对应的$N_p=6$，28，496，8128，…。

近代完全数的概念已推广为多倍完全数：对自然数 n，若 $\sigma(n)=kn$，k 是自然数，则称 n 为 k 倍完全数。这样，古代的完全数相当于 $k=2$的情形。容易验证120和672二数都是3倍完全数。亦即，$\sigma(120)=360$，$\sigma(672)=3\times672$。我们用"p_k 数"来表示 k 倍完全数。于是

$$n=2178540=2^2\cdot3^2\cdot5\cdot7^2\cdot13\cdot19\Longrightarrow\sigma(n)=4n$$

n是一个 p_4数。尽管多年来多倍完全数一直受到人们的注意，但下面两个基本问题却还没有得到解答：

（1） 对于所有$k=2$，3，4，…是否有无限多个p_k数？并算出这些数。

（2） 是否存在奇p_k数？

下面介绍三个已解决的有趣的p_k数的小问题。

1° 若 n 是 p_3 数，并且不是 3 的倍数，则3n是p_4数。

证明 因为$\sigma(n)=3n$，$(3,n)=1$，所以

$$\sigma(3n)=\sigma(3)\sigma(n)=4\sigma(n)=4\times 3n$$

这就表明了$3n$是p_4数。

2° 若$3n$是p_{4k}数，$3\nmid n$，则n是p_{3k}数。

证明 因为$(3,n)=1$，$\sigma(3n)=\sigma(3)\sigma(n)=4\sigma(n)$，又因$\sigma(3n)=4k\times 3n$，所以

$$4\sigma(n)=4k(3n)\Longrightarrow\sigma(n)=3k\cdot n$$

这就表明了n是p_{3k}数。

3° 若n是p_3数，$3|n$，但$5\nmid n$，$9\nmid n$，则$45n$是p_4数。

证明 因为$\sigma(n)=3n$且$n=3k$，$3\nmid k$，所以

$$\sigma(n)=\sigma(3k)=\sigma(3)\sigma(k)=4\sigma(k)$$

由于3^3，5，k两两互素，所以

$$\begin{aligned}\sigma(45n)&=\sigma(3^3)\,\sigma(5)\,\sigma(k)=40\times 6\sigma(k)=60\times 4\sigma(k)\\&=60\sigma(n)=60\times 3n=180n=4(45n)\end{aligned}$$

故$45n$是p_4数。

定理8·9 任何p_5数都有5个以上不同的素因子

证明 设n是p_5数，其标准分解式是

$$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$$

由定理8·8的引理1及$\sigma(n)=5n$，得

$$\frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdot\frac{p_2^{\alpha_2+1}-1}{p_2-1}\cdots\frac{p_k^{\alpha_k+1}-1}{p_k-1}$$

$$=5p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$$

两端除以n得

$$\frac{p_1-(p_1^{\alpha_1})^{-1}}{p_1-1}\cdot\frac{p_2-(p_2^{\alpha_2})^{-1}}{p_2-1}\cdots\frac{p_k-(p_k^{\alpha_k})^{-1}}{p_k-1}=5$$

丢掉分子的负项，得到不等式

$$\frac{p_1}{p_1-1}\cdot\frac{p_2}{p_2-1}\cdots\frac{p_k}{p_k-1}>5$$

如果认为所有素数都已排成递增的次序，那末$\frac{p_i}{p_i-1}$这些因子的值就是严格递减序列$\frac{2}{1}$，$\frac{3}{2}$，$\frac{5}{4}$，$\frac{7}{6}$，$\frac{11}{10}$，…中的项。注意，这个序列任何五项的乘积，都小于头五项之积，不足五项之积，更小于头五项之积。但是头五项之积是$\frac{77}{16}<5$。因此要使上述不等式成立，所用到的素数一定不止五个，这就说明了 n 具有五个以上不同的素因子。

此外，下面再简单介绍几种数的概念：

一． 过剩数。1944年数学家爱多士（Erdös）和阿楼古拉（Alaoglu）定义了如下的过剩数概念：

自然数n，若对于一切$k<n$，都有

$$\frac{\sigma(n)}{n}>\frac{\sigma(k)}{k}$$

则称 n 为过剩数。

如，当 $n=1$，2，3，4，5 时，$\sigma(n)=1$，3，4，7，6 所以对应的$\frac{\sigma(n)}{n}=1$，$\frac{3}{2}$，$\frac{4}{3}$，$\frac{7}{4}$，$\frac{6}{5}$。于是，我们看出 2 和 4 是过剩数，3 和 5 不是。下面证明一个十分优美的结论：

定理8·10 存在无限多个的过剩数。

证明 我们把自然数 n 的因子按递增次序记为 $d_1=1$，$d_2,d_3,\cdots d_l=n$；于是$\frac{n}{d_1}$，$\frac{n}{d_2}$，…，$\frac{n}{d_l}$是 n 的因子按递减次序的排列。它们的和相同，所以

$$\sigma(n)=\sum_{d_i\mid n}\frac{n}{d_i}\Longrightarrow\frac{\sigma(n)}{n}=\sum_{d_i\mid n}\frac{1}{d_i}$$

这是 n 的诸因数的倒数之和。

当 n 遍历自然数1，2，3，…时，它可以取一切阶乘 m! 的值。如果 $n=m!$ ，那末 n 的因数就包括1，2，…，m 的全体，且可能还有很多别的因子，所以

$$\frac{\sigma(n)}{n}=\sum_{d_i\mid n}\frac{1}{d_i}\geqslant\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{m}$$

这是著名的调和级数的部分和，当 m 无限增加，它是无限递增的。即，当 n 遍历所有自然数时$\frac{\sigma(n)}{n}$的值无限增大。若把$\frac{\sigma(n)}{n}$记作 u_n，则序列$u_1,u_2,\cdots,u_n,\cdots$无上界。因此，会不断地出现$u_n$，使得对一切$k<n$，都有 $u_n>u_k$，这样的 n 就是过剩数。这里所谓“不断地”系指这样的 n 有无限多个存在。因为不然的话，序列$u_1,u_2,\cdots,u_n,\cdots$就变成有上界了，这是不可能的。

这个定理的证明所用的知识十分初等，结论又十分优美。

二、实用数　1948年斯列尼瓦生（A.K.Srinivasan）定义实用数如下：

若自然数n，对所有的 $k\leqslant n$的k都是 n 的某些不同的真因子之和，则称 n 为实用数。

所有偶完全数，都是实用数。更一般地有

定理8·11　一切形如　$m=2^{n-1}(2^n-1)$的数，都是实用数。

证明　m的真因子包括下面两组数：

(A)　1，2，2^2，2^3，…，2^{n-1}，

(B)　2^n-1，$2(2^n-1)$，$2^2(2^n-1)$，…，$2^{2n-2}(2^n-1)$。

若 2^n-1 不是素数，而是合数，则还有一些真因子。但是只

要用（A）、（B）中的真因子就可以把其中某些适当的因子加起来，得到小于或等于m的所有的k。

下面分三种情况来讨论：

（1） 若$k\leqslant 2^{n-1}$，则 k 是（A）中某些数之和。事实上，若把 k 表成二进位数时，显然

$k=a_0+a_1 2+a_2 2^2+\cdots+a_{n-1}2^{n-1}$（$a_i=0$或1）取$a_i=1$的数加起来就得到 k了。

（2） 若$k=m$，则k是（A）和（B）中所有各数之和。这一点的证明是简单的只要把两个几何级数加起来就可以了。

（3） 若$2^{n-1}<k<m$，则以2^n-1作除数，得

$$k=(2^n-1)q+r\ (0\leqslant r<2^n-1)$$

其中$q<2^{n-1}$，否则$k\geqslant m$，这是不可能的。因此，由(1)知 q是（A）中某些数之和，r 也是（A）中某些数之和。由于（A）中的数都小于2^n-1，即（A）中的数都小于（B）中的任意一个数。而$(2^n-1)q$是（B）中若干个不同的数之和，故 k 可以表成（A）与（B）中若干不同的数的和。

更简单的，可以把 q 及 r 用 2 进位数来表示，并应用（B）中任一数都比（A）中任意数大，立即可得上述結论。

三 几乎完全数。几乎完全数就是盈数中盈余最小的数。即$\sigma(n)-2n$之值为最小，取其等 1，于是几乎完全数是指$\sigma(n)=2n+1$。换句话说，当 n 刚好等于它的一切非当然因子之和时，称 n 为几乎完全数。它可表示为

$$n=\sigma(n)-n-1.$$

但至今尚未发现任何几乎完全数。

和几乎完全数密切相关的是短缺最小的数即最接近于完全数的亏数。

$$\sigma(n)=2n-1\Longrightarrow n=\sigma(n)-n+1.$$

容易看出2^n($n=1, 2, 3, \cdots$)是这种数．事实上

$$\sigma(2^n)=1+2+\cdots+2^n=2^{n+1}-1=2\cdot 2^n-1,$$

$$\therefore \quad 2^n=\sigma(2^n)-2^n+1$$

四　半完全数．若自然n等于它的某些真因数之和，则称n为半完全数．如，$12=6+4+2$，故12是半完全数．显然半完全数不能是亏数；任何完全数都是半完全数；任何几乎完全数都是半完全数．看来，盈数多半是半完全数，例外的情形是很少见的，所以不是半完全数的盈数又叫做“怪数”．三个最小的怪数是70，836和4030，至今尚未发现任何奇数的怪数．不过已经知道怪数的数目是无限的*．

第四节　素数分布概况

素数的分布的状况，是数论中最有趣的一个分支．从经验中人们提出了许多猜测和定理，研究这些问题的方法亦是丰富多采的．

本节仅对素数分布的情况作最初步的介绍，为此先复习：

一、　无穷大的阶．在讨论素数分布的情况时，诸无穷大量比较的概况是读者必须了解的知识．为此我们先简单介绍无穷大的概念和性质，并引用下列符号表示量的变化状态．

---

* 怪数的研究是Pennsylvania州立大学的Stan Benkoski开创的，他和Paul Erdos合作即将发表的一篇文章表明，怪数序列具有正的Schnirelmann密度（一个自然数序列的Schnirelmann密度是$A(n)/n$的下确界，$A(n)$表示该序列中不大于n的各项的项数．一个序列若不含1，它的密度是0，为了避免这种情况，通常把数1添加到本来不包含1的序列里，对于怪数序列必须如此，奇数序列的密度是1/2，而平方数、素数以及2的方次幂序列的密度都是0。）这就表明用怪数来筛自然数，这个筛子比素数或其他密度为0的序列，稍微“密”一些。

≪，O，o，～

在给定的某过程中有一个量 x，如果不管正数 A 多么大，在这个过程中都可以找到这样一个时刻，使得在这个时刻后永远有 $|x|>A$，我们就说量 x 是（这个过程中的）一个无穷大量。

例如，如果整数 n 无限地增大，则 $(-1)^n 2^n$ 是一个无穷大量。因为任给 $A>0$，存在 N，当 $n>N$ 时，都有 $|(-1)^n 2^n|=2^n>A$。这说明了无穷大量可以在过程中多次改变它的符号。

又如，$(1+\alpha)^n$，$\alpha>0$。当 $n\to\infty$ 时是一个无穷大量。

1° 一个无穷大量与另一个有界量的和是一个无穷大量。

但必须注意，两个无穷大量之和，并不一定是一个无穷大量。如，当 $n\to\infty$ 时，两个无穷大量 $(-1)^n 2^n$ 与 $(-1)^{n+1} 2^n$ 之和就不是一个无穷大量了。

2° 两个无穷大量之积，还是无穷大量。

3° 有限个无穷大量之积，还是无穷大量。

4° 如果 x 是一个从来不等于 0 的无穷小量，那么 $\frac{1}{x}$ 是无穷大量。反之，若 x 是一个从来不等于 0 的无穷大量，则 $\frac{1}{x}$ 是一个无穷小量。

设 $f(x)$ 是任一函数，而 $\varphi(x)$ 是一正值函数（x 可取值正整数 n，趋向无穷；或 x 为一连续变数趋向无穷）。而 $f(x)/\varphi(x)$ 是一个有界量，即可以找到一个正数 A，使得

$$|f(x)|\leqslant A\varphi(x)$$

对于 x 的充分大值都成立，这时，我们就说，当 $x\to\infty$ 时

$$f(x)=O(\varphi(x)) \text{ 或 } f(x)\ll\varphi(x)\text{。}$$

若对两个函数 $f(x)$，$g(x)$ 与正值函数 $\varphi(x)$ 当 $x\to\infty$ 时，有

$$|f(x)-g(x)|\leqslant A\varphi(x),$$

那么我们就说 $x\to\infty$ 时，$f(x)-g(x)\ll\varphi(x)$ 或

$$f(x)=g(x)+O(\varphi(x))$$

例如，$\sin x\ll 1$ 或 $\sin x=O(1)$；$x\sin x\ll x$ 或 $x\sin x=O(x)$；$x+\sin x=x+O(1)$；$\sqrt{ax^2+b}\ll x$ 或 $\sqrt{ax^2+b}=O(x)$。而 $x+\frac{1}{x}\ll x\ll x+\frac{1}{x}$。

若 $\frac{f(x)}{\varphi(x)}$ 是一个无穷小量，即

$$\lim_{x\to\infty}\frac{f(x)}{\varphi(x)}=0$$

那么我们就说，当 $x\to\infty$ 时，

$$f(x)=o(\varphi(x)).$$

若

$$\lim_{x\to\infty}\frac{f(x)}{\varphi(x)}=1$$

则

$$f(x)\sim\varphi(x)$$

例如，$x+\frac{1}{x}=o(x^2)$，$x+\sin x\sim x$。

当然可以把"趋向无穷"换作"趋向于极限1"。

例如，当 $x\to 0$ 时，$x^2=o(x)$，$\sin x\sim x$，$1+x\sim 1$ 等等。但以后没有特别声明，都指趋向无穷。

它们有如下诸性质：

(i) $\varphi\ll\varphi$；$\varphi\sim\varphi$；$\varphi=o(\varphi)$。

(ii) $f\ll\varphi,\varphi\ll\psi\Longrightarrow f\ll\psi$；$f=O(\varphi),\varphi=o(\psi)$ $\Longrightarrow f=o(\psi)$

(iii) $f \ll \varphi, g \ll \psi \Longrightarrow f+g \ll \varphi+\psi$及 $f_g \ll \varphi\psi$；

$f=o(\varphi), g=o(\psi) \Longrightarrow f+g=o(\varphi+\psi)$及

$f_g=o(\varphi\psi)$。

(iv) $\varphi \sim \psi \Longrightarrow \psi \sim \varphi$； $\varphi \sim \psi, \psi \sim \chi \Longrightarrow \varphi \sim \chi$。

(v) $\varphi \sim \psi, \varphi_1 \sim \psi_1 \Longrightarrow \varphi\varphi_1 \sim \psi\psi_1$。

(vi) $\varphi=o(\psi) \Longrightarrow \varphi+\psi \sim \varphi$； $\psi>0$ 且 $\varphi+\psi \sim \varphi$

$\Longrightarrow \varphi=o(\psi)$。

下面再举一些例子。例如，若 x 是一个无穷小量，则

$x^2=o(x), x=o(1), 1-\omega x=o(x)$； $5x+3x^2=O(x)$，

$2\sin x=O(x)$； $x+3x^2 \sim x$等等。

若 x 是一个无穷大量，则

$x=o(x^2)$， $5x+3x^2=O(x^2)$， $1=o(x)$， $x^2+x \sim x^2$。

若 x 是有界量，则 $x=O(1)$。

二 对数函数（logarithmic function）

在素数分布的研究中，对数函数$\ln x$的知识是必不可少的。为此这里对它的一些知识作简单的介绍，而定义和一些初等性质当作读者已知的。因为

$$e^x=1+x+\cdots+\frac{x^n}{n!}+\frac{x^{n+1}}{(n+1)!}+\cdots$$

$$x^{-n}e^x=x^{-n}+x^{-(n-1)}+\cdots+\frac{1}{n!}+\frac{x}{(n+1)!}+\cdots$$

所以当 $x\to\infty$时，

$$x^{-n}e^x>\frac{x}{(n+1)!}\to\infty \tag{39}$$

即e^x趋向于无穷的速度较x的任何方次更快，或者说e^x的无穷大的阶大于x^n的阶。即

$$x^n=o(e^x) \tag{40}$$

若α是正实数，则

$$x^{\alpha}=O(x^{[\alpha]+1})=o(e^{x}) \tag{41}$$

因为 $\ln x$ 是e^x的反函数，以 $\ln y$代(41)的 x 得

$$(\ln y)^{\alpha}=o(y) \tag{42}$$

即得

$$\ln x=o(x^{\delta})\ (\delta>0) \tag{43}$$

换言之，$\ln x$的无穷大的阶，此 x 的任何正数方次为小，显然 $\ln\ln x$的无穷大的阶比 $\ln x$更小。

定理8·12 $$\sum_{n=1}^{x}\frac{1}{n}\sim\ln x \tag{44}$$

证明 $\because$ $\ln x=\int_1^x\frac{dt}{t}\leqslant\sum_{n=1}^{x}\frac{1}{n}\leqslant 1+\int_1^x\frac{dt}{t}=1+\ln x,$

$\therefore$ $$\sum_{n=1}^{x}\frac{1}{n}\sim\ln x$$

定理8·13 令

$$\operatorname{li} x=\lim_{\eta\to 0}\left(\int_0^{1-\eta}+\int_{1+\eta}^{x}\right)\frac{dt}{\ln t},$$

则

$$\operatorname{li} x\sim\frac{x}{\ln x} \tag{45}$$

证明

$\because$ $$\lim_{x\to\infty}\frac{\operatorname{li}x}{\frac{x}{\ln x}}=\lim\frac{(\operatorname{li}x)'}{\left(\frac{x}{\ln x}\right)'}=\lim\frac{\frac{1}{\ln x}}{\frac{1}{\ln x}-\frac{1}{\ln^2 x}}=1$$

$\therefore$ $$\operatorname{li}x\sim\frac{x}{\ln x}$$

三、$\pi(x)$的估值

用$\pi(x)$来表示不大于 x 的素数的个数，则有下表：

x	$\pi(x)$	$\frac{x}{\ln x}$	$\mathrm{li}\,x$	$\frac{\pi(x)}{\mathrm{li}\,x}$	$\frac{\pi(x)}{x}$
1,000	168	145	178	0.94…	0.1680
10,000	1,229	1,086	1,246	0.98…	0.1229
50,000	5,133	4,621	5,167	0.993…	0.1026
100,000	9,592	8,686	9,630	0.996…	0.0959
500,000	41,538	38,103	41,606	0.9983…	0.0830
1,000,000	78,498	72,382	78,628	0.9983…	0.0785
2,000,000	148,933	137,848	149,055	0.9991…	0.0745
5,000,000	348,513	324,149	348,638	0.9996…	0.0697
10,000,000	664,579	620,417	664,918	0.9994…	0.0665
20,000,000	1,270,607	1,189,676	1,270,905	0.9997…	0.0635
90,000,000	5,216,954	4,913,897	5,217,810	0.99983…	0.0580
100,000,000	5,761,455	5,428,613	5,762,209	0.99986…	0.0576
1,000,000,000	50,847,478	48,254,630	50,849,235	0.99996…	0.0508

观察上表，可以得到如下的启示：

（1） 素数的个数是无穷的（定理1·14），即当 $x\to\infty$ 时，$\pi(x)\to\infty$。

（2） 与整个正整数的个数之比，素数是少得多的．也可以说，几乎所有的整数都是合数．即

当 $x\to\infty$ 时，$\dfrac{\pi(x)}{x}\to 0$。

（3） 素数个数的无穷大的阶与li x十分接近．即 $\pi(x)\sim \mathrm{li}\ x\sim\dfrac{x}{\ln x}$．当然（3）包含了（1）和（2）。

（4） li x可作为π(x)的最佳渐近式。

（5） $\pi(x)<\mathrm{li}\ x$。

第五点并不真实，这一点已由里特伍德（Littlewood）证明了．（4）之讨论十分精深，必须在解析数论的专著中才能证明。

π(x)可表示为：$\pi(x)=\sum\limits_{p\leqslant x}1$．下面主要证明，π(x)与 $\dfrac{x}{\ln x}$ 是同阶无穷大．即存在两个正数 A_1 及 A_2，使得不等式

$$A_1\frac{x}{\ln x}<\pi(x)<A_2\frac{x}{\ln x}\quad(x\geqslant 2)\tag{46}$$

成立，或者说

$$\frac{x}{\ln x}\ll\pi(x)\ll\frac{x}{\ln x}\tag{46$'$}$$

这就是古典素数论中著名的切贝谢夫（Чебышев）定理。

定理8·14 设k是大于2的任一整数，则在自然数列中一定有两个相邻的素数p与p′（p′<p），使得 $p-p'\geqslant k$。

证明 令$m=k!+2$，则$2|m$，$(2+1)|(m+1)$，…，$k|(m+k-2)$。又因$k>2$，故$m>2$，$m+1>3$，…，$m+k-2>k$，而$m,m+1,\cdots,m+k-2$是$k-1$个连续合数。设p'是小于m的最大素数，则大于p'且与p'相邻的素数p，就是大于$m+k-2$的最小素数，故有

$$p'\leqslant m-1,\ p\geqslant m+k-1\Longrightarrow p-p'\geqslant(m+k-1)-(m-1)=k$$

由定理8·14知道，相邻两个素数之间的“距离”可以无限增大。另一方面，又存在下列素数对：

3，5；5，7；11，13；17，19；29，31；41，43；101，103；107，109；137，139；…；10016957,10016959；…；10^9+7，10^9+9；…它们都是距离为2的素数对。这样的素数对称为孪生素数（prime twins），这样的最大素数对，今已知道的是

1,000,000,009,649和1,000,000,009,651这样的素数对很可能有无穷多个，这个猜测亦尚未解决（见第一章第五节）。又如，

5，7，11；11，13，17；17，19，23；…；101，103，107；…；10014491，10014493，10014497；…

都是素数。因此有人猜测有无穷多组素数p，$p+2$，$p+6$。这些例子说明了，从整个素数的数列来看，其分布情况是很不规则的，人们如何从中发现一些分布的规律是很有意义的课题，这个问题首先应归功于切贝谢夫。

引理1 若n是任一正整数，且

$$N=\frac{(2n)!}{(n!)^2}$$

则

$$(\pi(2n)-\pi(n))\ln n \leqslant \ln N \leqslant \pi(2n)\ln 2n$$

证明 设

$$N=\prod_{p_i\leqslant 2n} p_i^{\alpha_i}$$

是N的标准分解式，则由[n]函数的性质(viii)，知道

$$\alpha_i=\sum_{r=1}^{\infty}\left[\frac{2u}{p_i^r}\right]-2\sum_{r=1}^{\infty}\left[\frac{n}{p_i^r}\right]$$

$$=\sum_{r=1}^{\left[\frac{\ln 2n}{\ln p_i}\right]}\left(\left[\frac{2n}{p_i^r}\right]-2\left[\frac{n}{p_i^r}\right]\right)$$

(因为当 $r>\left[\frac{\ln 2n}{\ln p_i}\right]$ 时，$p_i^r>2n>n$)。由于 $0\leqslant\left[\frac{2n}{p_i^r}\right]-2\left[\frac{n}{p_i^r}\right]\leqslant 1$。故

$$\alpha_i\leqslant\sum_{r=1}^{\left[\frac{\ln 2n}{\ln p_i}\right]} 1=\left[\frac{\ln 2n}{\ln p_i}\right]\leqslant\frac{\ln 2n}{\ln p_i}$$

$$\therefore\quad \ln N=\sum_{p_i\leqslant 2n}\alpha_i\ln p_i\leqslant\sum_{p_i\leqslant 2n}\ln 2n=\pi(2n)\ln 2n$$

另一方面，若 $n<p\leqslant 2n$，则 $p\mid(2n)!$，$(p,n!)=1$，因而 $p\mid N$，故

$$\ln N\geqslant\sum_{n<p\leqslant 2n}\ln p>\ln n\sum_{n<p\leqslant 2n}1=$$

$$=(\pi(2n)-\pi(n))\ln n$$

这就是证明了所要的结论。

现在来估计ln N。即

引理2 若n，N的意义同引理1．则

$$n\ln 2\leqslant\ln N\leqslant 2n\ln 2$$

证明 因为N是$(1+x)^{2n}$的展开式中x^n的系数，故

$$N\leqslant(1+1)^{2n}=2^{2n}$$

另一方面，

$$N=\frac{2n(2n-1)\cdots(n+1)}{n!}$$

$$=2\left(2+\frac{1}{n-1}\right)\cdots\left(2+\frac{n-1}{1}\right)\geqslant 2^n$$

把上两式取对数，即得引理的结论。

定理8·15 当 $x\geqslant 2$ 时，

$$\frac{1}{5}\cdot\frac{x}{\ln x}<\pi(x)\leqslant 5\frac{x}{\ln x} \tag{47}$$

证明 (i) 当 $n\geqslant 6$时，令 $n=\left[\frac{x}{2}\right]$，则 $x\geqslant 2n$，$n>\frac{x}{3}$。因而由引理1，2，即得

$$\pi(x)\ln x\geqslant\pi(2n)\ln 2n\geqslant\ln N\geqslant n\ln 2>\frac{\ln 2}{3}x>\frac{1}{5}x$$

又由于$\frac{x}{\ln x}$在区间〔2，6〕中的最大值是$\frac{6}{\ln 6}$，因此当$2\leqslant x\leqslant 6$时，

$$\frac{1}{5}\frac{x}{\ln x}\leqslant\frac{1}{5}\frac{6}{\ln x}^{*}<1\leqslant\pi(2)\leqslant\pi(x)$$

即(47)中前一个不等式成立。

(ii) 由引理1，2，知

$$(\pi(2n)-\pi(n))\ln n\leqslant\ln N\leqslant 2n\ln 2$$

以 $n=2^r$代入上式，即得

$$r(\pi(2^{r+1})-\pi(2^r))\leqslant 2^{r+1}$$

---

* 因为 $\ln 2=0.69315$，$\ln 8=1.09861$，$\ln 6=1.79176$，所以 $\frac{1}{5}\frac{6}{\ln 6}<\frac{1.5}{1.79176}<1$。

由于$\pi(2^{r+1})\leqslant 2^r$，故有

$$(r+1)\pi(2^{r+1})-r\pi(2^r)\leqslant 2^{r+1}+\pi(2^{r+1})\leqslant 3\cdot 2^r$$

任意给定一个正整数m，把 $r=0, 1, \cdots, m-1$依次代入上式，得到m个不等式，把它们两边相加，即得

$$m\pi(2^m)\leqslant 3(1+2+\cdots+2^{m-1})<3\times 2^m$$

当 $n\geqslant 2$ 时，有一确定的正整数m，使得$2^{m-1}\leqslant x<2^m$，于是$\frac{1}{m}<\frac{\ln 2}{\ln x}$，所以

$$\pi(x)\leqslant\pi(2m)\leqslant\frac{1}{m}\cdot 3\cdot 2^m\leqslant 6\cdot\ln 2\cdot\frac{x}{\ln x}\leqslant 5\frac{x}{\ln x}$$

故(47)中后一个不等式亦成立。定理得证。

这个定理实际是给出了，切贝谢夫不等式(46)中$A_1=\frac{1}{5}$，$A_2=5$ 的情况。由定理8·15，立即得到

系 几乎所有的正整数都是合数，即

$$\lim_{x\to\infty}\frac{\pi(x)}{x}=0$$

由于定理8·15中，x 可以是正实数，并不限制 x 为正整数，所以系里的 x 亦可看作是通过实数而趋于无穷。

勒让得和高斯猜测的素数的进一步性质，即著名的素数定理（prime number theorem）：

$$\lim_{x\to 8}\frac{\pi(x)}{\frac{x}{\ln x}}=1$$

这个猜测，直到1896年，才由法国数学家阿达玛(Hadamard)和得拉魏力泊桑（de la Vallée poussin）同时互相独立地用深邃的复变函数的理论来证明。1949年，赛尔伯格（Selberg）和爱多士（Erdös）才分别给出了素数定理的初等证明（参考华罗庚著《数论导引》第九章）。

中国数学家华罗庚和吴方给出了比素数定理更精确的对$\pi(x)$的估值。若用函数

$$\mathrm{Li}\,x=\int_2^x \frac{dt}{\ln t}$$

代替$\frac{x}{\ln x}$，可以得到

$$|\pi(x)-\mathrm{Li}\,x|\leqslant Bxe^{-A(\ln x)^{\frac{4}{7}}\cdot(\ln\ln x)^{-\frac{1}{7}}}$$

目前更准确的结论是

$$|\pi(x)-\mathrm{Li}\,x|\leqslant Bxe^{-A(\ln x)^{\frac{3}{5}}\cdot(\ln\ln x)^{-\frac{3}{5}}}$$

式中A代表某一适当小的正常数，B代表某一充分大的常数。这在目前是最好的结果。理想的结果是尚待证明的猜测：

$$|\pi(x)-\mathrm{Li}\,x|\leqslant Bx^{\frac{1}{2}+\varepsilon}$$

其中B是充分大的常数，ε是任意小的正常数。

四、贝特朗（Bertrand）假设

这个假设的证明首先由切贝谢夫给出。

定理8·16 贝特朗假设（Bertrand's postulate）。对任一实数$x\geqslant1$，在$(x, 2x)$中必有一素数。

为了证明上述结论，先证

引理1 当$n\geqslant5$时，

$$\frac{1}{2n}2^{2n}<C_{2n}^{n}<\frac{1}{4}2^{2n} \tag{49}$$

证明 $\because$ $2nC_{2n}^{n}=\frac{2}{1}\cdot\frac{3}{1}\cdot\frac{4}{2}\cdot\frac{5}{2}\cdots\frac{2n-2}{n-1}\cdot\frac{2n-1}{n-1}\cdot$

$$\cdot\frac{2n}{n}\cdot\frac{2n}{n}>2^{2n}$$

$$\therefore \qquad \frac{1}{2n}2^{2n} < C_{2n}^{n}$$

用数学归纳法证明(49)的右边不等式

A， 当$n=5$时，显然有

$$C_{10}^{5}=252<256=\frac{1}{4}\cdot 2^{10}$$

B， 设$C_{2n}^{x}<\frac{1}{4}2^{2n}$，则

$$C_{2(n+1)}^{n+1}=\frac{(2n)!(2n+1)(2n+2)}{(n!)^2(n+1)(n+1)}<4C_{2n}^{n}<$$

$$<\frac{1}{4}2^{2(n+1)}$$

引理2 设$b\geqslant 10$，则

$$\prod_{10<p\leqslant b} p<2^{2b} \tag{50}$$

证明 用$\{\xi\}$表示$\geqslant\xi$的最小整数，且令

$$a_1=\left\{\frac{b}{2}\right\},\quad a_2=\left\{\frac{b}{2^2}\right\},\quad \cdots=,\quad a_k\left\{\frac{b}{2^k}\right\},\quad \cdots$$

则 $a_1\geqslant a_2\geqslant\cdots\geqslant a_k\geqslant\cdots$，并且

$$a_k<\frac{b}{2^k}+1=2\frac{b}{2^{k+1}}+1\leqslant 2a_{k+1}+1$$

由于两端都是整数，故有

$$a_k\leqslant 2a_{k+1} \tag{51}$$

设m是使$a_m\geqslant 5$的最大整数，即$a_{m+1}<5$。又由(51)得$a_m<10$，因$2a_1\geqslant b$，故m个隔间

$$a_m<\eta\leqslant 2a_m,\quad a_{m-1}<\eta\leqslant 2a_{m-1},\quad\cdots,\quad a_1<\eta\leqslant 2a_1$$

整个地掩盖了隔间$10<\eta\leqslant b$，故

$$\prod_{10<p\leqslant b} p\leqslant \prod_{a_1<p\leqslant 2a_1} p \prod_{a_2<p\leqslant 2a_2} p\cdots \prod_{a_m<p\leqslant 2a_m} p$$

由引理 1 知道

$$\prod_{n<p\leqslant an} p < C_{2n}^{n} < 2^{2(n-1)}$$

$$\therefore \quad \prod_{10<p\leqslant b} p \leqslant 2^{2(a_1-1+a_2-1+\cdots+a_m-1)}$$

$$< 2^{2\left(\frac{b}{2}+\frac{b}{2^2}+\cdots+\frac{b}{2^m}\right)} < 2^{2b}$$

这就证明了引理 2 。

引理3 证明：

$$\prod_{n<p\leqslant 2n} p \mid C_{2n}^{n} \text{ 且 } C_{2n}^{n} \mid \prod_{p^r\leqslant 2n<p^{r+1}} p^r \qquad (52)$$

证明 因为素数 p 满足 $n<p\leqslant 2n$ 时，$p\mid(2n)!$ ，但 $p\nmid n!$ ，故 $p \parallel C_{2n}^{n}$，

$$\therefore \quad \prod_{n<p\leqslant 2n} p \mid C_{2n}^{n}$$

在C_{2n}^{n}中 p 的方次数为

$$\sum_{m=1}^{r}\left(\left[\frac{2n}{p^m}\right]-2\left[\frac{n}{p^m}\right]\right)\leqslant r$$

这里的 r 是使不等式 $p^r\leqslant 2n<p^{r+1}$成立的自然数。上式左边的每一项皆$\leqslant 1$，故

$$C_{2n}^{n} \mid \prod_{p^r\leqslant 2n<p^{r+1}} p^r$$

这就证明了(52)的后一式。

引理4 若 p 是素数，且$p>\sqrt{2n}$，则$p^2\nmid C_{2n}^{n}$ 。

证明 由(52)的后一式知道 p在C_{2n}^{n}的标准分解式中出

现的次数 r，最大的可能是 $p^r \leqslant 2n$，而 $p^2 > 2n$，所以

$$p^2 \nmid C_{2n}^n$$

引理5 当 $n \geqslant 3$ 时，适合$\frac{2}{3}n < p \leqslant n$ 的素数p，则 $p \nmid C_{2n}^n$。

证明 因为$2n < 3p \leqslant 3n$，所以在$(2n)!$中仅能出现p和2p二因子，但$(n!)^2$中出现 p^2因子，因此在$C_{2n}^n = \frac{(2n)!}{(n!)^2}$中不可能出现 p 的因子。即

$$p \mid c_{2n}^n$$

引理 5 是证明定理的主要依据。

定理8·16的证明 由上面诸引理知道，在c_{2n}^n中出现的素因数 p 有

$$C_{2n}^n \leqslant \prod_{p \leqslant \sqrt{2n}} p^r \prod_{\sqrt{2n} < p \leqslant \frac{2}{8}n} p \prod_{n < p \leqslant 2n} p$$

$$\leqslant \prod_{p \leqslant \sqrt{2n}} (2n) \prod_{\sqrt{2n} < p \leqslant \frac{2}{8}n} p \prod_{n < p \leqslant 2n} p$$

由(49)及(50)及上式知道，当 $n \geqslant 50$ 时（即$\sqrt{2n} \geqslant 10$时），

$$2^{2n} < 2nC_{2n}^n < 2n^{\sqrt{2n}+1} \prod_{\sqrt{2n} < p \leqslant \frac{2}{8}n} p \prod_{n < p \leqslant 2p} p <$$

$$< (2n)^{\sqrt{2n}+1} 2^{\frac{4}{8}n} \prod_{n < p \leqslant 2n} p \qquad (53)$$

今用反证法，若在 n 与2n之间无素数，则

$$2^{2n} < (2n)^{\sqrt{2n}+1} 2^{\frac{4}{3}n} \Longrightarrow 2^{\frac{2}{3}n} < (2n)^{\sqrt{2n}+1} \qquad (54)$$

当 n 充分大时，显然(54)是不成立的。

今具体算出(54)成立的确切范围。

(i) 当 $n \geqslant 1$ 时，$n \leqslant 2^{n-1}$。事实上，当 $n=1$，2 时，$n=2^{n-1}$，当 $n=3$ 时，$3<2^2$；可设 $n \leqslant 2^{n-1}$，则 $n+1 \leqslant 2^{n-1}+1 < 2^{n-1}+2^{n-1}=2^n\ (n>2)$。

(ii) 当 $n \geqslant 50$时，由(i)得

$$2n=(\sqrt[6]{2n})^6 < ([\sqrt[6]{2n}]+1)^6 \leqslant 2^{([\sqrt[6]{2n}]+1-1)\cdot 6}$$

$$=2^{6[\sqrt[6]{2n}]} \leqslant 2^{6\sqrt[6]{2n}} \qquad (55)$$

由(54)，(55)及 $18 \leqslant 2\sqrt{2n}\ (n \geqslant 50)$ 知

$$2n < (2n)^{3(1+\sqrt{2n})} < \left(2^{6\sqrt[6]{2n}}\right)^{3(1+\sqrt{2n})}$$

$$=2^{\sqrt[6]{2n}(18+18\sqrt{2n})} < 2^{\sqrt[6]{2n}\times 20\sqrt{2n}} = 2^{20(2n)^{\frac{2}{3}}}$$

上不等式的指数有 $2n < 20(2n)^{\frac{2}{3}} \Longrightarrow (2n)^{\frac{1}{3}} < 20 \Longrightarrow n < \frac{1}{2}\cdot 20^3 = 4000$ 的关系，也就是说(54)仅当 $n<4000$ 时才可能成立。故当 $n \geqslant 4000$ 时，必有一个素数 p，适合于 $n < p \leqslant 2n$。

(iii) 当$n<4000$时，因为一串素数

2，3，5，7，13，23，43，83，163，317，631，1259，2503，4001． (56)

后一个素数都小于前一个的二倍．对于任一 $n, 1 \leqslant n < 4000$，都可在(56)中取得一个大于 n 的最小素数 p，p′表示p的的前一项，则

$$p' \leqslant n < p \leqslant 2p' \leqslant 2n$$

因而定理得证。

这个定理实际上有一个等价命题

系 若 p_r 是第 r 个素数，则对任意的 r 都有

$$p_{r+1} < 2p_r$$

对于定理8·16，有的书里（如H.W.的《An introduction to the theory of numbers 定理418）先证明当 $n > 2^9 = 512$ 时，必存在素数 p，满足

$$n < p \leqslant 2n$$

而后证明 $n \leqslant 512$ 的情况其证法同(iii)。

下面将对 $[n, 2n]$ 里素数的数目作一估计。

定理8·17 当 $n \geqslant 1$ 时，则有二正常数 α 和 β，使

$$\alpha \frac{n}{\ln n} < \pi(2n) - \pi(n) < \beta \frac{n}{\ln n} \tag{57}$$

证明 从(48)中知道，取 $\beta = 2$ 就得到(57)右边的不等式。

由(53)和(55)知，当 $n \geqslant 4000$（当 $n < 4000$ 时，定理显然成立）时，

$$\prod_{n<p\leqslant 2n} p > 2^{2n-\frac{4}{3}n}(2n)^{-(1+\sqrt{2n})}$$

$$> 2^{\frac{2n}{3}} 2^{-6\sqrt[6]{2n}(1+\sqrt{2n})} = 2^{\frac{1}{3}(2n-\sqrt[6]{2n}(18+18\sqrt{2n}))}$$

$$> 2^{\frac{1}{3}(2n-19(2n)^{\frac{2}{3}})} \geqslant 2^{\frac{2}{3}n(1-\frac{19}{20})} = 2^{\frac{1}{30}n}$$

由上式及

$$\prod_{n<p\leqslant 2n} p < (2n)^{\pi(2n)-\pi(n)}$$

可得

$$2^{\frac{1}{30}n} < (2n)^{\pi(2n)-\pi(n)}$$

$$\Longrightarrow \frac{1}{30}n\ln 2 < [\pi(2n)-\pi(n)]\ln 2n$$

$$\Longrightarrow \pi(2n)-\pi(n) > \frac{\ln 2}{30}\cdot\frac{n}{\ln 2n} > \frac{\ln 2}{60}\cdot\frac{n}{\ln n}$$

$$(\because 2\ln n > \ln 2n)$$

取$\alpha=\frac{\ln 2}{60}$即得(57)左边的不等式

定理8·16虽已证实了贝特朗猜测的真确性，但此定理的精确度不高，精确度更高的结论已超出本书的范围。有人猜测：在 n^2 与 $(n+1)^2$ 之间必有一素数存在。这是一个尚未解决的问题。

五、切贝谢夫定理。这是初等数论的一条比较重要的定理。它表明了 $\pi(x)$ 与$\frac{1}{2}$，$\frac{1}{3}$，…，$\frac{1}{n}$的平均值的倒数同阶。即

定理8·18　设$H(n)=\sum\limits_{t=2}^{n}\frac{1}{t}$，当 $n\geqslant 2$ 时，则

$$\frac{1}{8}\leqslant \pi(x)\frac{H(n)}{n} < 6$$

证明本定理之前，先证三个引理。

引理1　当 $k\geqslant 0$ 时，有

$$\pi(2^{k+1})\leqslant 2^k$$

证明　由于大于 2 的偶数都是合数，9，15，21等也是合数，故当 $x>9$时，$\pi(x)\leqslant\frac{x}{2}$。又

$$\pi(2)=1=2^0,\quad \pi(4)=2=2^1,\quad \pi(8)=4=2^2$$

引理2　当 $l>0$ 时，有

$$\frac{1}{2}l\leqslant H(2^l)\leqslant l$$

证明　因为

$$H(2^l)=\frac{1}{2}+\left(\frac{1}{3}+\frac{1}{4}\right)+\left(\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}\right)+\cdots$$

$$+\left(\frac{1}{2^{l-1}+1}+\cdots+\frac{1}{2^l}\right)\geqslant\frac{1}{2}+\left(\frac{1}{2^2}+\frac{1}{2^2}\right)$$

$$+\left(\frac{1}{2^3}+\frac{1}{2^3}+\frac{1}{2^3}+\frac{1}{2^3}\right)+\cdots+\left(\frac{1}{2^l}+\cdots+\right.$$

$$\left.+\frac{1}{2^l}\right)=\frac{1}{2}l$$

$$H(2^l)=\left(\frac{1}{2}+\frac{1}{3}\right)+\left(\frac{1}{4}+\frac{1}{5}+\frac{1}{6}+\frac{1}{7}\right)+\cdots+\frac{1}{2^l}\leqslant$$

$$\leqslant\left(\frac{1}{2}+\frac{1}{2}\right)+\left(\frac{1}{4}+\frac{1}{4}+\frac{1}{4}+\frac{1}{4}\right)+\cdots$$

$$+\left(\frac{1}{2^{l-1}}+\cdots+\frac{1}{2^{l-1}}\right)+\frac{1}{2^l}\leqslant l .$$

$$\therefore\qquad \frac{1}{2}l\leqslant H(2^l)\leqslant l$$

引理3

$$\prod_{n<p\leqslant 2n}p\,\Big|\,C_{2n}^{n}\ \text{且}\ C_{2n}^{n}\,\Big|\prod_{p^r\leqslant 2n<p^{r+1}}p^r \tag{58}$$

证明　因为$C_{2n}^{n}=\dfrac{(2n)!}{n!n!}$，而在（$n$，$2n$）中的素数 $p\mid(2n)!$但 $p\nmid n!$，故(58)的第一式成立。

在c_{2n}^{n}中 p 之方次数为

$$\sum_{m=1}^{r}\left(\left[\frac{2n}{p^m}\right]-2\left[\frac{n}{p^m}\right]\right)\leqslant r\ (p^r\leqslant 2n<p^{r+1})$$

因其中的每一项皆$\leqslant 1$。故得(58)的后一式。

定理8·18的证明： 由引理3知道

$$n^{\pi(2n)-\pi(n)}<\prod_{n<p\leqslant 2n} p\leqslant C_{2n}^{n}\leqslant \prod_{p^r\leqslant 2n<p^{r+1}} p^r\leqslant$$

$$\leqslant (2n)^{\pi(2n)} \quad (n\geqslant 1) \tag{59}$$

又因

$$C_{2n}^{n}=\frac{2n(2n-1)\cdots(n+1)}{n(n-1)\cdots 1}$$

$$=2\left(2+\frac{1}{n-1}\right)\cdots\left(2+\frac{v}{n-v}\right)\cdots\left(2+\frac{n-1}{1}\right)\geqslant 2^n$$

且

$$C_{2n}^{n}\leqslant(1+1)^{2n}=2^{2n}$$

故由(59)可知

$$n^{\pi(2n)-\pi(n)}<2^{2n},\quad 2^n\leqslant(2n)^{\pi(2n)} \quad (n\geqslant 1) \tag{60}$$

令 $n=2^k$，$k=0$，1，2，…，可得

$$2^{k(\pi(2^{k+1})-\pi(2^k))}<2^{2^{k+1}}$$

$$2^{2^k}\leqslant 2^{(k+1)\pi(2^{k+1})} \quad (k\geqslant 0)$$

即得

$$k\left(\pi(2^{k+1})-\pi(2^k)\right)<2^{k+1},\quad 2^k\leqslant(k+1)\pi(2^{k+1}) \tag{61}$$

由(61)及引理1，得

$$(k+1)\pi(2^{k+1})-k\pi(2^k)<2^{k+1}+\pi(2^{k+1})\leqslant 3\cdot 2^k \ (k\geqslant 0)$$

取 $k=0$，1，2，…，k，而将所得的诸式相加，得

$$(k+1)\pi(2^{k+1})<3(2^0+2^1+\cdots+2^k)<3\cdot 2^{k+1} \ (k\geqslant 0) \tag{62}$$

由(61)及(62)，得

$$\frac{1}{2}\frac{2^{k+1}}{k+1}\leqslant\pi(2^{k+1})<3\frac{2^{k+1}}{k+1}\quad(k\geqslant 0)\tag{63}$$

令 n 是大于等于 2 的整数，选取k使

$$2^{k+1}\leqslant n<2^{k+2}\quad(k\geqslant 0)\tag{64}$$

由(64)，(63)及引理 2，得

$$\pi(n)\leqslant\pi(2^{k+2})<3\frac{2^{k+2}}{k+2}\leqslant 6\frac{2^{k+1}}{H(2^{k+2})}\leqslant 6\frac{n}{H(n)}\tag{65}$$

及

$$\pi(n)\geqslant\pi(2^{k+1})\geqslant\frac{1}{2}\frac{2^{k+1}}{k+1}=\frac{1}{8}\frac{2^{k+2}}{\frac{1}{2}(k+1)}$$

$$\geqslant\frac{1}{8}\frac{2^{k+2}}{H(2^{k+1})}\geqslant\frac{1}{8}\frac{n}{H(n)}\tag{66}$$

(65)，(66)二式对 $n\geqslant 2$ 都真。故

$$\frac{1}{8}\leqslant\pi(n)\frac{H(n)}{n}<6$$

定理8·19 当 $n\geqslant 2$ 时，有

$$\frac{1}{8}\leqslant\frac{\pi(n)}{\frac{n}{\ln n}}\leqslant 12\tag{67}$$

证明 当 $n\geqslant 2$ 时，

$$\ln\frac{n}{2}=\int_2^n\frac{dt}{t}<\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}=H(n)<\int_1^n\frac{dt}{t}=\ln n$$

由定理8·18及上式，得

$$\frac{1}{8}\leqslant\frac{\pi(n)}{\frac{n}{H(n)}}<\frac{\pi(n)}{\frac{n}{\ln n}}$$

当 $n\geqslant 4$ 时，由

$$\ln\frac{n}{2}\geqslant\frac{1}{2}\ln n$$

可得

$$6>\pi(x)\frac{\ln\frac{n}{2}}{n}>\pi(x)\frac{\frac{1}{2}\ln n}{n}$$

从而得

$$\frac{\pi(x)}{\frac{n}{\ln n}}>12.$$

当 $n=2$，3的情况，因为

$$\frac{1}{2}\ln3=0.5493<\frac{1}{2}+\frac{1}{3}=H(3),$$

$$\frac{1}{2}\ln2=0.3466<\frac{1}{2}=H(2),$$

所以上式对 $n\geqslant2$ 都成立。

六　表示素数的函数

定理8·20　有一个实数 α 存在，若令

$$\alpha=\alpha_0,\ 2^{\alpha_0}=\alpha_1,\ \cdots,\ 2^{\alpha_n}=\alpha_{n+1},\ \cdots$$

则 $[\alpha_n]$ 常为一素数。

证明　今用归纳法作一素数的数列 $\{p_n\}$：取 $p_1=3$，由定理8·16知道有一素数 p_{n+1} 适合

$$2^{p_n}<p_{n+1}<p_{n+1}+1\leqslant2^{p_n+1}$$

若 $p_{n+1}+1=2^{p_n+1}$，则 $p_{n+1}=2^{p_n+1}-1$ 不是素数，因为它有 $2^{\frac{1}{2}(p_n+1)}-1$ 的因数。故

$$2^{p_n}<p_{n+1}<p_{n+1}+1<2^{p_n+1}$$

作以 2 为底的对数，并定义

$$\log^{(n)}x=\log^{(n-1)}(\log x)$$

作数列

$$u_n=\log^{(n)}p_n,\quad v_n=\log^{(n)}(p_n+1)$$

$\because\quad p_n<\log p_{n+1}<\log(p_{n+1}+1)<p_n+1$

$$\Longrightarrow u_{n+1}=\log^{(n+1)}p_{n+1}=\log^{(n)}\log p_{n+1}>\log^{(n)}p_n=u_n$$

且

$$v_n=\log^{(n)}(p_n+1)>\log^{(n)}\log(p_{n+1}+1)=\log^{(n+1)}(p_{n+1}+1)=v_{n+1}.$$

即 u_n是一个递增序列，v_n是一个递减序列，故有一实数α存在，使得

$$\lim_{n\to\infty}u_n=\alpha \text{ 且} u_n<\alpha<v_n$$

亦即

$$p_n<\alpha_n<p_n+1$$

$$\therefore\quad [\alpha_n]=p_n$$

常为一素数，其中$\alpha_n=2^{\alpha_{n-1}}$

七　等差级数中的素数

在第一章习题18中曾证明了形如4n－1的素数有无穷多个。一般地，若（a,b）＝1，则形如 $an+b(n\geq0)$ 的素数的个数是无穷的，这是著名的狄里赫来（Dirichlet）定理。其证明方法比较复杂，这里不作介绍，读者若有兴趣可参考华罗庚著《数论导引》第九章。下面仅证明它的一些特例。

可设 a>0，b>0。若能证明，对任意这样的a,b，都有一个 an＋b（n>0）的素数存在，则狄里赫来定理已证明。事实上，若有一个正整数 n，使得

$$an+b=p_1(>b)$$

为素数；次以ap_1代替 a，又有一个正整数 n_1，使得

$$ap_1n_1+b=p_2(>p_1)$$

为素数，$p_2=a(p_1n_1)+b$ 亦是 $an+b$ 形的素数。依此类推，则形如 $an+b$ 的素数的个数无穷。

定理8·21 若 $k>1$，则有无穷多个形如 $kn+1$ 的素数存在。

由前面的分析，要证明本定理，只要证明：$\forall k\in N$，$k>1$都有形如 $kn+1$的素数存在就可以了。

因为 $e^{2\pi i\frac{t}{k}}$，$t=0, 1, \cdots, k-1$ 是方程$x^k=1$的 k个根，令

$$F_n(x)=\prod_{(t,\ n)=1}(x-e^{2\pi i\frac{t}{n}})$$

这个乘积中的 t 为过模 n的互素剩余系。显然，若 n 为过模 k 的一切正因子时

$$x^k-1=\prod_{n|k}F_n(x)$$

事实上，上式右边的每一个根都是左边的根，反之，左边的每一个根亦是右边的根，且无重复（根据定理 3·6系2知道$\sum_{n|k}\varphi(n)=k$，所以上式两边根的个数是相等的）。如，当$k=6$时，$F_1(x)=x-1$，$F_2(x)=x+1$，$F_3(x)=(x-e^{\frac{2}{3}\pi i})(x-e^{\frac{4}{3}\pi i})=x^2+x+1$，$F_6(x)=(x-e^{\frac{1}{3}\pi i})(x-e^{\frac{5}{3}\pi i})=x^2-x+1$，故 $x^6-1=F_1(x)F_2(x)F_3(x)F_6(x)$。令

$$x^k - 1 = F_k(x)G_k(x)$$

其中$G_k(x)$是诸多项式$x^n - 1$（$n|k$，$n<k$）的最小公倍式。并且是整系数多项式*。如，$k=6$时，$G_6(x) = [x-1, x^2-1, x^3-1] = (x-1)(x+1)(x^2+x+1)$，而$F_6(x) = x^2 - x - 1$。

若整数$x \neq \pm 1$，则整数

$$F_k(x)G_k(x) \neq 0$$

为了证明本定理，先证

引理1 若$1<n<k$，$n|k$，整数$x \neq \pm 1$，则

$$\left(x^n - 1, \frac{x^k-1}{x^n-1}\right) \Big| k$$

证明 设$k = nd$，$x^n - 1 = y$，则

$$\frac{x^k-1}{x^n-1} = \frac{(y+1)^d - 1}{y} = y^{d-1} + c_d^1 y^{d-2} + \cdots + c_d^2 y + d$$

$$\equiv d \pmod{y}$$

$$\therefore \quad \left(x^n - 1, \frac{x^k-1}{x^n-1}\right) = (y, ty+d) = s \Longrightarrow s|d \Longrightarrow s|k$$

引理2 若整数$x \neq \pm 1$，则$F_k(x)$及$G_k(x)$的公共素因子，必为k的因子。

证明 假定素数$p|(F_k(x), G_k(x))$，则由

$$p|G_k(x) \Longrightarrow p\Big|\prod_{\substack{n|k\\ n<k}} F_n(x) \Longrightarrow \text{存在 } n, n|k, n<k \text{ 使得}$$

$$p|F_n(x) \Longrightarrow p|x^n - 1; \qquad (68)$$

---

* 高斯（Gauss）定理：设$f(x)$是一个整系数多项式，若

$$f(x) = g(x)h(x)$$

这里$g(x)$，$h(x)$是二有理系数多项式，则有一个有理数γ，使

$$\varphi(x) = \gamma g(x), \quad \psi(x) = \frac{1}{\gamma} h(x)$$

都是整系数。即$f(x) = \varphi(x)\psi(x)$为二整系数多项式之积。

次由

$$p \mid F_k(x) \Longrightarrow p \mid \frac{x^k-1}{x^n-1} \Longrightarrow p \mid \left(x^n-1, \frac{x^k-1}{x^n-1} \right)$$

（(68)中的n）从而由引理1知 $p \mid k$。

定理8·21的证明：令 $x = ky$，则

$$F_k(x)\, G_k(x) = x^k - 1 = (k\,y)^k - 1 \equiv -1 \pmod k \tag{69}$$

可以选择适当的 y，使得

$$F_k(x) \neq \pm 1$$

因为 $F_k(x) = \pm 1$ 只有有限个根，故这种选择是可能的。

$F_k(x)$ 中至少有一个素因子 p，p 不是 $G_k(x)$ 的因子，否则由引理2知 $F_k(x)$ 的一切素因子都是 k 的因子，此与(69)的结论矛盾。换言之，对于任一 k 的真因子 n，都有适当的 x，使

$$x^n \not\equiv 1 \pmod p \tag{70}$$

但是

$$x^k \equiv 1 \pmod p \tag{71}$$

现在证明 $k \mid p-1$。若不然，便有二整数 s 和 t 存在，使得

$$(k, p-1) = sk + t(p-1)$$

即对于 $n = (k, p-1)$，则由费马定理及(71)，得

$$x^n = x^{sk+t(p-1)} = (x^k)^s \cdot (x^{p-1})^t \equiv 1 \pmod p$$

这与(70矛盾。即 $p \equiv 1 \pmod k$，亦即有一形如 $kn+1$ 的素数存在。这就证明了定理。

习　　题

1. 证明：一个完全数或盈数 n 的任何倍数 mn，m≥2．都是盈数。

2. 证明：亏数的任何因子都是亏数。

3. 证明：若p是素数，则p^a是亏数。

4. 证明：σ(n)是奇数的充要条件是 n 为平方数或二倍平方数。

5. 欧拉定理：任一奇完全数一定具有形状$n = p^{4\alpha+1}\cdot q^2$，(p，q) = 1，p是奇素数。

6. 证明：形如①6n－1，②8n＋5的素数是无穷的。

7. 若x≥a时，f(x)是一个递增非负函数，则当 ξ≥a 时，常有

$$\left|\sum_{a\leqslant n\leqslant\xi} f(n) - \int_a^\xi f(x)dx\right| \leqslant f(\xi)$$

8. 证明：$n^{n-1}e^{-n+1} \leqslant n! \leqslant n^{n+1}e^{-n+1}$.

9. 黎曼ζ函数（Riemann Zeta function）指的是和式

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}\ (s>1)^{*} \qquad (1)$$

更一般的 $s = \sigma + it$（$\sigma > 1$ 和t是实数）．则

(i) $$\zeta'(s) = -\sum_{n=1}^{\infty} \frac{\ln n}{n^s}(s>1) \qquad (2)$$

---

* 如 $\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$，一般地，对正整数 n，ξ(2n) 是 π^{2n} 的倍数。如，$\zeta(4) = \frac{1}{90}\pi^4$。一般地

$$\zeta(2n) = \frac{2^{2n-1}B^n}{(2n)!}\pi^{2n},$$

其中B_n是贝努利（Bernoulli）数。

(ii) $\zeta(s) = \prod_p \frac{1}{1-p^{-s}}$ (3)

(iii) $\zeta(s) = \frac{1}{s-1} + O(1)$ (4)

(iv) $\ln\xi(s) = \ln\frac{1}{s-1} + O(s-1)$ (5)

(v) $\zeta'(s) = -\frac{1}{(s-1)^2} + O(1)$ (6)

第九章　二元二次型

本章主要介绍二元二次型的基础知识，证明了判别式 $d=b^2-4ac$ 是相似变换下的不变量，并探讨了同一 d 的二次型的分类问题。引进并借助克朗里克符号讨论了 $x^2\equiv d \pmod{4k}$ 的解数。在第三节对斐尔（Pell）方程的最小解也作了初步的介绍。最后还给出一般二元二次不定方程的解法以及计算二次曲线上整点的数目的简单方法。

第一节　二元二次型的分类

定义9·1　给定整数 a，b，c，二次齐次多项式

$$F=F(x,\ y)=ax^2+bxy+cy^2 \tag{1}$$

叫做二元二次型（binary quadric(quadratic) form），或简称为型（form）。以 $\{a,\ b,\ c\}$ 表示之，整数

$$d=b^2-4ac$$

叫做型(1)的判别式（discriminant）。

注意本章所指的整数都指有理整数。当 b 是偶数时，$d\equiv0 \pmod 4$；当 d 是奇数时，$d\equiv1 \pmod 4$。

定理9·1　F可分解成二整数系数的一次式之积的充要条件是 d 为一整数的平方。

证明　(i)　若 $d=k^2$ 且 $a\neq0$，则

$$ax^2+bxy+cy^2=a\left[\left(x+\frac{b}{2a}y\right)^2-\frac{k^2}{4a^2}y^2\right]$$

$$=a\left(x+\frac{b-k}{2a}y\right)\left(x+\frac{b+k}{2a}y\right)$$

$$= \frac{1}{4a}[2ax + (b-k)y][2ax + (b+k)y]$$

若 $a=0$，则$F=(bx+cy)y$。

(ii)　若 $ax^2+bxy+cy^2=(rx+sy)(tx+uy)$，则

$a=rt$，$b=st+ru$，$c=su \Longrightarrow d=b^2-4ac$

从而　$d=b^2-4ac=(st+ru)^2-4rt\cdot su$

$\quad\quad =(st-ru)^2$

下面假设 d 不是平方数。

(1)　若 $d<0$，$a>0$，则

$$4aF=(2ax+by)^2+(4ac-b^2)y^2$$

$$=(2ax+by)^2-dy^2 \tag{2}$$

因为$-d>0$，所以对于任意整数x，y，都使$F(x, y)\geqslant 0$，当且仅当 $x=y=0$时，$F(0, 0)=0$。这种型称为定正型(Positive definite form)。

以-1乘定负型，即得定正型，故下面常讨论定正型，并简称为定型(definite form)。

(2)　若 $d>0$，则

$$F(1, 0)=a, \ F(b, -2a)=-da \tag{3}$$

若 $a\neq 0$，则(3)的二值一正一负；若 $c\neq 0$，则

$$F(0, 1)=c, \ F(-2c, b)=-dc \tag{3$'$}$$

的二值一正一负。

若 $a=c=0$时，$F(1, 1)=b$，$F(1, -1)=-b$，也是一正一负。故当 $d>0$时，型F能取正值也能取负值，因此称此型为不定型(indefinite form)。

定义9·2　若有一整系数变换

$$\begin{cases} x=rX+sY, \\ y=tX+uY, \end{cases} \quad ru-st=1 \tag{4}$$

即

$$\begin{pmatrix} x \\ y \end{pmatrix}=\begin{pmatrix} r & s \\ t & u \end{pmatrix}\begin{pmatrix} X \\ Y \end{pmatrix}, \quad \begin{vmatrix} r & s \\ t & u \end{vmatrix}=1 \qquad (4')$$

变F(x, y)为G(X, Y)，则称 F与G 相似（similar），记作

$$F\sim G$$

或称F经$\begin{pmatrix} r & s \\ t & u \end{pmatrix}$而变为G。

具体地，若要把F = {a, b, c}经变换 (4) 而变为G = {a_1, b_1, c_1}，则因

$$F=(x,\ y)\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}, \quad (x,\ y)=(X, Y)\begin{pmatrix} r & t \\ s & u \end{pmatrix}$$

$$\therefore\ G=(X,\ Y)\begin{pmatrix} r & t \\ s & u \end{pmatrix}\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}\begin{pmatrix} r & s \\ t & u \end{pmatrix}\begin{pmatrix} X \\ Y \end{pmatrix}$$

$$=(X,\ Y)\begin{pmatrix} ar^2+brt+ct^2 & ars+\frac{1}{2}b(ru+st)+ctu \\ ars+\frac{1}{2}b(ru+st)+ctu & as^2+bsu+cu^2 \end{pmatrix}\begin{pmatrix} X \\ Y \end{pmatrix}$$

$$=a_1X^2+b_1XY+c_1Y^2$$

其中

$$\begin{cases} a_1 = ar^2 + brt + ct^2 \\ b_1 = 2ars + b(ru + st) + 2ctu = 2ars + b(1 + 2st) \\ \qquad + 2ctu \\ c_1 = as^2 + bsu + cu^2 \end{cases} \tag{5}$$

由(5)及(4)即得

$$b_1^2 - 4a_1c_1 = b^2 - 4ac = d$$

从而得到

定理9·2 相似二型的判别式相等。

注意：定理9·2的逆命题不真。例如，{1，0，5}与{2，2，3}的判别式相等，但不相似，因为

$$\begin{cases} 2 = r^2 + 5t^2 \\ 2 = 2rs + 10tu \\ 3 = s^2 + 5u^2 \end{cases}$$

无满足 $ru - st = 1$的整数解。

又若 $d<0$，$a>0$，则 $a_1 = F(r, t)$ 是定正型的，故 $a_1>0$，所以G也是定正型的。同样地，若F是定负型的；则G也是定负型的；若F是不定型的，则 G 也是不定型的。故得

系 二元二次型经相似变换，不改变它所属的类型。

定理9·3 相似关系是一个等价关系，即它满足：

1°$F \sim F$；

2°$F \sim G \Longrightarrow G \sim F$；

3°$F \sim G$，$G \sim H \Longrightarrow F \sim H$

这个定理的证明十分简单，留给读者来完成。

从定理9·2及9·3知道，可把 d 相同的一切二元二次型依照相似来分类，同一类的诸型都相似，不同类的二型不相

似．此外，当同一类的诸型作为整数环上的二元二次函数时，它们的值域都相同．事实上，若$G\sim F$且$G(X,Y)=k$，则 $k=F(rX+sY,\ tX+uY)$．

下面将证明，这样的分类方法其类数是有限的．

定理9·4 若按相似关系把型分类，则每一类中至少有一型适合于

$$|b|\leqslant|a|\leqslant|c|$$

证明 因为同一类中的任意二型都相似，因此类中任一个型$\{a,b,c\}$的系数，都可以用另一个型$\{a_0,b_0,c_0\}$的系数按公式(5)表出，简称 a（或 b，c）可由$\{a_0,b_0,c_0\}$表出．

设$a\neq0$是此类诸型中x^2的系数中绝对值最小的一个，任给类中的一型$\{a_0,b_0,c_0\}$，则存在矩阵$T=\begin{pmatrix}r&s\\t&u\end{pmatrix}$，$|T|=1$，使得$\{a_0,b_0,c_0\}$经T变为$\{a,b',c'\}$，由(5)的第一式得

$$a=a_0r^2+b_0rt+c_0t^2$$

且$(r,t)=1$（因为$ru-st=1$）．再取矩阵

$$\begin{pmatrix}1&h\\0&1\end{pmatrix}$$

把$\{a,b',c'\}$变为$\{a,b,c\}$，由(5)的第二式得

$$b=2ah+b'$$

可取适当的整数 h，使得

$$|b|\leqslant|a|$$

事实上，当$a>0$时，要$a\geqslant b=2ah+b'\Longrightarrow h\leqslant\dfrac{a-b'}{2a}$的整数；当$a<0$时，要$a\leqslant b=2ah+b'\Longrightarrow h\geqslant\dfrac{a-b'}{2a}$的整数．

因为 $c\neq 0$（若 $c=0$，则 $d=b^2$ 是一个平方数，与假设矛盾），而 c 可由 $\{a, b', c'\}$ 表出，且 $\{a, b', c'\}$ 与 $\{a_0, b_0, c_0\}$ 属于同一类，此外 $\{a, b, c\}$ 经 $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ 变成 $\{c, -b, a\}$，然后由 $|a|$ 的最小性，可知 $|c|\geqslant|a|$。

$$\therefore \quad |b|\leqslant|a|\leqslant|c|$$

定理9·5 按相似关系把型分类，对于任一给定的 d，其类数是有限的。

证明 (i) 若 $d>0$（不定型），由定理9·4知

$$|ac|\geqslant b^2=d+4ac>4ac\Longrightarrow ac<0$$

又

$$4a^2\leqslant 4|ac|=-4ac=d-b^2\leqslant d\Longrightarrow |a|\leqslant\frac{\sqrt{d}}{2}$$

再从定理9·4知，$|b|\leqslant\frac{\sqrt{d}}{2}$，故 a 与 b 都只有有限个可能性。而 $c=\frac{b^2-d}{4a}$ 的值也只有有限个可能性。所以对给定的 d，其类数有限。

(ii) 若 $d\leqslant 0$（定型）。设 $a>0$，由定理9·4知

$$-d=4ac-b^2\geqslant 4a^2-b^2\geqslant 3a^2\Longrightarrow 0<a\leqslant\sqrt{\frac{|d|}{3}}$$

再由定理9·4知，a，b，c 都只有有限个可能性，所以对给定的 d 其类数有限。

定理9·6 $d=b^2-4ac<0$，$a>0$ 的型（定正型）的类数等于集合

$$-a<b\leqslant a<c \text{ 或 } 0\leqslant b\leqslant a=c \tag{6}$$

的整数组 $\{a, b, c\}$ 的组数。

证明 (i) 由定理9·4知道，在一类中至少有一型适合于

$$-a\leqslant b\leqslant a\leqslant c \tag{7}$$

因为定正型的 a，c 常为正，故(7)比(6)多出下列诸型：

$$-a=b,\ a<c;\ 及\ -a\leqslant b<0,\ a=c$$

下面证明

$$\{a,\ -a,\ c\}\sim\{a,\ a,\ c\}及\{a,\ -b,\ a\}\sim\{a,\ b,\ a\}$$

因为$\{a,\ -a,\ c\}$经$\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$而变为$\{a,\ a,\ c\}$；而$\{a,\ -b,\ a\}$经$\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$而变为$\{a,\ b,\ a\}$，故得任一类中必有一型适合(6)。

(ii) 今证明，其中任意两个适合(6)的不同的型都不相似．即要证明，若适合(6)的

$$\{a,\ b,\ c\}\sim\{a',\ b',\ c'\}$$

则 $a=a'$，$b=b'$，$c=c'$．

可设 $a'\leqslant a$，令$\begin{pmatrix}r & s\\ t & u\end{pmatrix}$变$\{a,\ b,\ c\}$为$\{a',\ b',\ c'\}$，由(5)得

$$a'=ar^2+brt+ct^2 \tag{α}$$

$$b'=2ars+b(ru+st)+2ctu \tag{β}$$

由(α)及(6)知

$$a\geqslant a'\geqslant ar^2-a|rt|+at^2=a(|r|-|t|)^2+a|rt|\geqslant a|rt| \tag{γ}$$

$$\therefore\qquad |rt|\leqslant 1$$

若$|rt|=1$，则 $a=a'$；否则，则 $rt=0$，且 $r\neq 0$或 $t\neq 0$，此时

$$a\geqslant a'\geqslant a(r^2+t^2)\geqslant a\Longrightarrow a=a'$$

先设 $c>a$，则 $t=0$．否则，由于 $ct^2>at^2$，从(γ)得

$$a > ar^2 - a|rt| + at^2 = a(|r| - |t|)^2 + a|rt| \geqslant a,$$

即 $a > a$，这是不可能的。故 $t = 0$，$ru = 1$，由(β)得

$$b' = 2ars + b \equiv b \pmod{2a} \tag{δ}$$

又因 $-a < b \leqslant a$ 及 $-a = -a' < b' \leqslant a' = a$。因而 b，b'都是模 2a的绝对最小剩余且不等于 $-a$。于是，由(δ)知 $b = b'$。由(δ)左边知 $s = 0$，再由(5)的第三式知$c = c'$。

同样的方法，若 $c' > a'(=a)$，亦可得到 $b = b'$，$c = c'$。

最后，若 $a = a' = c = c'$，则

$$b = \pm b'$$

再由 $b \geqslant 0$，$b' \geqslant 0$，得 $b = b'$。

注：对于不定型的情况，证明比较困难，这里不作介绍。

由定理9·4知道每一类中总存在一个满足$|b| \leqslant |a| \leqslant |c|$的型$\{a, b, c\}$，由定理9·6知道在这样的型中有且只有一个满足条件(6)，我们把满足(6)的型叫做已化型（simplified form）。即每一个定正型的类中有且只有一个已化型。

例9·1 证明 $d = -48$，$a > 0$ 时，有且只有四个类。

证明 由定理9·5的证明(ii)中知道，当 $d = -48 < 0$，$a > 0$时，必有 $a \leqslant \sqrt{\frac{|d|}{3}} \doteq 4$。又由定理9·6及 $c = \frac{b^2 - d}{4a} \geqslant a$，得到下列四个已知型：

$\{1, 0, 12\}$，$\{2, 0, 6\}$，$\{3, 0, 4\}$，$\{4, 4, 4\}$

同样地，

例9·2 给出$0 < -d < 20$的一切已化型。

解 可按上例的方法把这些已化型列表于下：

d	−3	−4	−7	−8	−11	−12		−15		−16		−19	−20	
a	1	1	1	1	1	1	2	1	2	1	2	1	1	2
b	1	0	1	0	1	0	2	1	1	0	0	1	0	2
c	1	1	2	2	3	3	2	4	2	4	2	5	5	3

事实上，$d\equiv b^2 \pmod 4$，而$\{0\}$，$\{1\}$是模 4 的平方剩余；$\{2\}$，$\{3\}$是模 4 的平方非剩余。故满足$0<-d\leqslant 20$的$d=-3$，-4，-7，-8，-11，-12，-15，-16，-19，-20。

第二节　克朗里克符号

本节主要引入克朗里克符号，并应用它的性质来探讨二次同余式

$$x^2\equiv d \pmod{4k}$$

的解数，其中$k>0$，$(d, k)=1$。

定义9·3　设$d\equiv 0$或$1 \pmod 4$，且d不是平方数，$m>0$，定义克朗里克（Kronecker）符号$\left(\frac{d}{m}\right)$如下：

$\left(\frac{d}{p}\right)=$勒让得符号，若$p$是奇素数；

$$\left(\frac{d}{2}\right)=\begin{cases}1, & 若d\equiv 1 \pmod 8,\\ -1, & 若d\equiv 5 \pmod 8;\end{cases}$$

$$\left(\frac{d}{m}\right)=\prod_{r=1}^{k}\left(\frac{d}{p_r}\right), 若m=\prod_{r=1}^{k}p_r，p是素数。$$

从定义 9·3 可以看出，克朗里克符号是把第五章第三节的勒让得符号推广到$p=2$，并且当m为合数时，引用雅

可比符号且推广到 $p=2$（即允许 m 为偶数）。定义9·3 有下列性质：

1° $$\left(\frac{d}{m}\right)=\begin{cases}0, & 若(d,\ m)>1,\\ \pm 1, & 若(d,\ m)=1.\end{cases}$$

2° 若$m_1>0$，$m_2>0$，则

$$\left(\frac{d}{m_1m_2}\right)=\left(\frac{d}{m_1}\right)\left(\frac{d}{m_2}\right).$$

定理9·7 若 $m>0$，$(m,\ d)=1$，则克朗里克符号

$$\left(\frac{d}{m}\right)=\begin{cases}\left(\dfrac{m}{|d|}\right), & 若\ d\ 是奇数\\ \left(\dfrac{2}{m}\right)^b(-1)^{\frac{u-1}{2}\cdot\frac{m-1}{2}}\left(\dfrac{m}{|u|}\right), & 若 d=2^bu,\ 2\nmid u\end{cases} \tag{8}$$

其中$\left(\dfrac{m}{|d|}\right)$，$\left(\dfrac{2}{m}\right)$，$\left(\dfrac{m}{|u|}\right)$都是雅可比符号。

证明 (i) 若 d 是奇数，即 $d\equiv 1\pmod 4$。则由定义9·3，定理5·4及雅可比符号的性质3°，得

$$\left(\frac{d}{m}\right)=\begin{cases}(-1)^{\frac{m-1}{2}}(-1)^{\frac{4k+3-1}{2}\cdot\frac{m-1}{2}}\left(\dfrac{m}{|d|}\right)=\left(\dfrac{m}{|d|}\right), & 若\ d=4k+3,\ k\geqslant 0;\\ (-1)^{\frac{4k+1-1}{2}\cdot\frac{m-1}{2}}\left(\dfrac{m}{d}\right)=\left(\dfrac{m}{|d|}\right), & 若\ d=4k+1,\ k\geqslant 0.\end{cases}$$

当 $m=2^tv$ 是偶数时（$2\nmid v$，$t\geqslant 1$），则$\left(\dfrac{d}{2}\right)=\left(\dfrac{2}{d}\right)$。因为当 $d=8k+1$时，$\left(\dfrac{2}{d}\right)=\left(\dfrac{d}{2}\right)=1$；当 $d=8k+5$ 时，$\left(\dfrac{d}{2}\right)=\left(\dfrac{2}{d}\right)=-1$。

因而$\left(\frac{d}{m}\right)=\left(\frac{d}{2}\right)^t\left(\frac{d}{v}\right)=\left(\frac{2}{d}\right)^t\left(\frac{v}{|d|}\right)=\left(\frac{m}{|d|}\right)$.

综上所述，当 d 是奇数，(d, m) = 1时，

$$\left(\frac{d}{m}\right)=\left(\frac{m}{|d|}\right)$$

(ii) 若 $d=2^b u$，即 $d\equiv 0 \pmod 4$)，必有 $b\geqslant 2$，$2\nmid u$。因为(d, m) = 1，故 m 是奇数，又因 k 是整数时，$(-1)^{-k}=(-1)^k$，因而

$$\left(\frac{d}{m}\right)=\left(\frac{2}{m}\right)^b\left(\frac{u}{m}\right)=\begin{cases}\left(\frac{2}{m}\right)^b(-1)^{\frac{u-1}{2}\cdot\frac{m-1}{2}}\left(\frac{m}{|u|}\right), & \text{若 } u>0;\\ \left(\frac{2}{m}\right)^b(-1)^{\frac{u-1}{2}\left(1+\frac{-u-1}{2}\right)}\left(\frac{m}{|u|}\right) & \\ =\left(\frac{2}{m}\right)^b(-1)^{\frac{u-1}{2}\cdot\frac{m-1}{2}}\left(\frac{m}{|u|}\right), & \text{若 } u<0\end{cases}$$

这就证明了本定理。

系 当m>0，(d, m) = 1时，

$$\left(\frac{d}{m}\right)=\left(\frac{d}{m+|d|}\right)$$

证明 当d是奇数时，由定理9·7知，$\left(\frac{d}{m}\right)=\left(\frac{m}{|d|}\right)=\left(\frac{m+|d|}{|d|}\right)$，而$\left(\frac{d}{m+|d|}\right)=\left(\frac{m+|d|}{|d|}\right)$，所以

$$\left(\frac{d}{m}\right)=\left(\frac{d}{m+|d|}\right)$$

当 $d=2^b u$ 为偶数时，其中 $b\geqslant 2$，$2\nmid u$，此时 m 为奇

数。而由定理7·9知，$\left(\frac{d}{m}\right)=\left(\frac{2}{m}\right)^{b}(-1)^{\frac{u-1}{2}\cdot\frac{m-1}{2}}\left(\frac{m}{|u|}\right)$

$=(-1)^{\frac{m^2-1}{8}b}(-1)^{\frac{u-1}{2}\cdot\frac{m-1}{2}}\left(\frac{m}{|u|}\right)$。所以

$$\left(\frac{d}{m+|d|}\right)=\left(\frac{2}{m+|d|}\right)^{b}(-1)^{\frac{u-1}{2}\cdot\frac{m+|d|-1}{2}}\left(\frac{m+|d|}{|u|}\right)$$

$$=(-1)^{\frac{(m+|d|)^2-1}{8}b}(-1)^{\frac{u-1}{2}\cdot\frac{m-1}{2}}\left(\frac{m}{|u|}\right)$$

因为$\frac{(m+|d|)^2-1}{8}b=\frac{m^2-1}{8}b+(2^{b-2}|u|m+2^{2b-3}u^2)b$ $(b\geqslant 2)$，右边后一项一定是偶数。

$$\therefore\quad \left(\frac{d}{m}\right)=\left(\frac{d}{m+|d|}\right)$$

此系更一般地说明了“分母”用关于模$|d|$与 m 同余的任一数代替 m 时，克朗里克符号的值不变。

由定理6·7及定理7·9的系，立即得到

定理9·8 克朗里克符号$\left(\frac{d}{m}\right)$是模$|d|$的一个特征函数。

定理9·9 设 $m>0$，$n>0$，$m\equiv -n(\bmod |d|)$，则

$$\left(\frac{d}{m}\right)=\begin{cases}\left(\frac{d}{n}\right), & 若\ d>0;\\ -\left(\frac{d}{n}\right), & 若\ d<0.\end{cases}\tag{10}$$

证明 因为

$$\left(\frac{d}{m}\right)=\left(\frac{d}{n|d|-n}\right)=\left(\frac{d}{n(|d|-1)}\right)=\left(\frac{d}{n}\right)\left(\frac{d}{|d|-1}\right),$$

故当 n 为奇数时，由定理9·7，得

$$\left(\frac{d}{|d|-1}\right)=\left(\frac{|d|-1}{|d|}\right)=\left(\frac{-1}{|d|}\right)=(-1)^{\frac{|d|-1}{2}}$$

$$=\begin{cases}1, & 若\ d>0;\\ -1, & 若\ d<0.\end{cases}$$

而当 d 为偶数时，令 $d=2^b u$，$2\nmid u$，$b\geqslant 2$，则由定理 9·7，得

$$\left(\frac{d}{|d|-1}\right)=\left(\frac{2}{|d|-1}\right)^b(-1)^{\frac{u-1}{2}(2^{b-1}|u|-1)}\left(\frac{|d|-1}{|u|}\right)$$

$$=(-1)^{\frac{(2^b|u|-1)^2-1}{8}b}(-1)^{\frac{u-1}{2}}\left(\frac{-1}{|u|}\right)$$

$$=(-1)^{\frac{u-1}{2}}\left(\frac{-1}{|u|}\right)=(-1)^{\frac{u-1}{2}+\frac{|u|-1}{2}}$$

$$=\begin{cases}1, & 若\ d>0;\\ -1, & 若\ d<0.\end{cases}$$

故得定理。

定理9·10 设 $k>0$，$(d, k)=1$，同余式

$$x^2\equiv d(\bmod 4k), \tag{11}$$

的解数等于

$$2\sum_{f|k}\left(\frac{d}{f}\right).$$

其中 f 为过 k 的一切不包含平方因子的正因子。

证明 (i) 若 d 为奇数，即 $d\equiv 1(\bmod 4)$ 且 $(d, k)=1$，则 $(d, 4k)=1$。设 $4k=2^{\alpha}p_1^{\alpha_1}\cdots p_k^{\alpha_k}$，令 $2=p_0$，$\alpha=\alpha_0$，由定理4·8知，(11)等价于同余式组

$$x^2\equiv d(\bmod p_i^{\alpha_i})(i=0, 1, \cdots, k) \tag{11'}$$

且若T_i表示(11′)的第 i 个方程的解数，则(11)的解数$T=T_0T_1\cdots T_k$。又由定义9·3及定理5·6、5·7知道，(11′)各同余式的解数为

$$T_i=\begin{cases}2, & 若\ p_i=2,\ \alpha_i=2;\\ 2\left(1+\left(\frac{d}{p_i}\right)\right), & 若\ p_i=2,\ \alpha_i>2;\\ 1+\left(\frac{d}{p_i}\right), & 若\ p_i>2.\end{cases}$$

$$\therefore\quad T=2\prod_{p\mid k}\left(1+\left(\frac{d}{p}\right)\right)=2\sum_{f\mid k}\left(\frac{d}{f}\right)$$

(ii) 设 d 为偶数，则$d\equiv0\pmod 4$。故 k 为奇数，而

$$x^2\equiv d\equiv0\pmod 4$$

有二解；

$$x^2\equiv d\left(\bmod p_i^{\alpha_i}\right)$$

有$1+\left(\frac{d}{p_i}\right)$个解。

$$\therefore\quad T=2\prod_{p\mid k}\left(1+\left(\frac{d}{p}\right)\right)=2\sum_{f\mid k}\left(\frac{d}{f}\right)$$

显然，若 x 是(11)的一个解，则 x＋2k 也是(11)的一个解，并且

$$x+2k\not\equiv x\pmod{4k}$$

所以有

系 (11)中增加条件$0\leqslant x<2k$后，(11)的解数等于$\sum_{f\mid k}\left(\frac{d}{f}\right)$。

第三节　形如$x^2-dy^2=l$的二次不定方程

本节主要讨论形如

$$x^2-dy^2=l,\ 0<|l|<\sqrt{d} \tag{12}$$

其中d是非平方的正整数的不定方程的整数解的问题，以及裴尔（Pell）方程的最小整数解的问题。

定理9·11　若把$\sqrt{d}$化成连分数

$$\sqrt{d}=[a_1,\ a_2,\ \cdots,\ a_n,\ \alpha_n]$$

则存在二整数p_n，q_n，使得

$$\alpha_n=\frac{\sqrt{d}+p_n}{q_n},\ p_n^2\equiv d(\bmod\ q_n)$$

证明　今用数学归纳法证明之。

A）　当$n=1$时，$a=[\sqrt{d}]$，$\alpha_1=\dfrac{1}{\sqrt{d}-[\sqrt{d}]}=$

$=\dfrac{\sqrt{d}+[\sqrt{d}]}{d-[\sqrt{d}]^2}$，即$p_1=[\sqrt{d}]$，$q_1=d-[\sqrt{d}]^2$都是整数，且$p_1^2\equiv d(\bmod q_1)$。

B）　设存在二整数p_n，q_n使得

$$\alpha_n=\frac{\sqrt{d}+p_n}{q_n},\ p_n^2\equiv d(\bmod q_n)$$

由于$\alpha_n=a_{n+1}\dfrac{1}{\alpha_{n+1}}$，今要证，存在二整数$p_{n+1}$，$q_{n+1}$使得

$$\frac{\sqrt{d}+p_n}{q_n}=a_{n+1}+\frac{q_{n+1}}{\sqrt{d}+p_{n+1}}\text{及}\ d-p_{n+1}^2$$

$$\equiv 0(\bmod q_{n+1}) \tag{a}$$

亦即只要证，存在二整数 p_{n+1}，q_{n+1} 使得

$$d + p_n p_{n+1} = a_{n+1} q_n p_{n+1} + q_n q_{n+1} \tag{b}$$

$$p_n + p_{n+1} = a_{n+1} q_n \tag{c}$$

$$d - p_{n+1}^2 \equiv 0 \pmod{q_{n+1}} \tag{a}$$

$(b) - p_{n+1} \times (c)$ 得

$$d - p_{n+1}^2 = q_n q_{n+1} \equiv 0 \pmod{q_{n+1}} \tag{d}$$

因为适合(d)的 p_{n+1}，q_{n+1} 亦适合(a)，且 $p_{n+1}(c) + (d)$ 就得到等式(b)，所以只需证明有二整数 p_{n+1}，q_{n+1} 适合(c)、(d)就可以了。

由(c)知道，应取 $p_{n+1} = a_{n+1} q_n - p_n$，并且有

$$p_n^2 \equiv p_{n+1}^2 \pmod{q_n}$$

由归纳法假设，由 $d - p_n^2 \equiv 0 \pmod{q_n}$ 得到 $d - p_{n+1}^2 \equiv 0 \pmod{q_n}$，从而存在 q_{n+1} 使得 $d - p_{n+1}^2 = q_{n+1} q_n$。

这就证明了所要的结论。

定理9·12 二次不定方程

$$x^2 - dy^2 = (-1)^n q_n \tag{12}$$

都有解，其中 q_n 是定理9·11中所定义的。

若 $l \neq (-1)^n q_n$，且 $|l| < \sqrt{d}$，则

$$x^2 - dy^2 = l \tag{13}$$

没有解。

证明 由第一章等式(8)知道

$$\sqrt{d} = \frac{\alpha_n P_n + P_{n-1}}{\alpha_n Q_n + Q_{n-1}} = \frac{P_n(\sqrt{d} + p_n) + P_{n-1} q_n}{Q_n(\sqrt{d} + p_n) + Q_{n-1} q_n}$$

由于 $\sqrt{d}$ 是无理数，故得

$$P_n = Q_n p_n + Q_{n-1} q_n \tag{e}$$

$$dQ_n = P_n p_n + P_{n-1} q_n \tag{f}$$

$P_n(e) - Q_n(f)$得

$$P_n^2 - dQ_n^2 = (P_n Q_{n-1} - P_{n-1} Q_n) q_n = (-1)^n q_n$$

即$\sqrt{d}$的第 n 个渐近分数的分子与分母(P_n, Q_n)是(12)的一个解。这就证明了定理的前一部分。

由定理1·6的系知

$$\alpha = \frac{P_n}{Q_n} + \frac{(-1)^{n-1}\varepsilon_n'}{Q_n^2} \Longrightarrow \frac{(-1)^{n-1}\varepsilon_n'}{Q_n^2}$$

$$= \frac{(-1)^{n-1}}{Q_n(Q_n\alpha_n + Q_{n-1})} \tag{g}$$

其中$\frac{P_n}{Q_n} = [a_1, \cdots, a_n]$是$\alpha$的第 n 个渐近分数。并且由$Q_n > Q_{n-1} (n = 2, 3, \cdots)$，得

$$\frac{Q_n}{Q_n + Q_{n-1}} > \frac{1}{2} \Longrightarrow \left|\alpha - \frac{P_n}{Q_n}\right| < \frac{1}{2Q_n^2} \tag{h}$$

为了证明定理的后一部分，先证

(i) 若实数

$$\alpha = \frac{P_n\beta + P_{n-1}}{Q_n\beta + Q_{n-1}} = [a_1, \cdots, a_n, \beta] \tag{i}$$

中的$\frac{P_n}{Q_n}$是α的渐近分数，则其充要条件是：$\beta \geqslant 1$。

当$\beta \geqslant 1$时，显然P_n/Q_n是α的第 n 个渐近分数，且$\beta = \alpha_n = [a_{n+1}, a_{n+2}, \cdots]$。

若$0 < \beta < 1$，则

$$\left[a_n + \frac{1}{\beta}\right] = a_n + c, \quad c \geqslant 1$$

即

$$\alpha=[a_1, \cdots, a_n+c, \cdots]$$

故$\frac{P_n}{Q_n}=[a_1, \cdots, a_n]$不是$\alpha$的渐近分数，所以(i)中$\frac{P_n}{Q_n}$是$\alpha$的渐近分数的充要条件是$\beta\geqslant1$．换句话说，可把$\beta\geqslant1$改写为

(ii) 若$\frac{p}{q}=[a_1, \cdots, a_n]=\frac{P_n}{Q_n}$，且

$\delta\varepsilon_n=q^2\alpha-pq$，$\delta=(-1)^{n-1}$，$0<\varepsilon_n<1$

则$\frac{p}{q}$是α的渐近分数的充要条件是

$$\varepsilon_n\leqslant\frac{Q_n}{Q_n+Q_{n-1}}$$

并且由(h)知道，若有一有理数$\frac{p}{q}$，满足

$$\left|\alpha-\frac{p}{q}\right|<\frac{1}{2q^2}$$

则$\frac{p}{q}$必为α的一个渐近分数。

(iii) 由定理的前一部分知道，当$l=(-1)^nq_n$时，(12)有解(P_n, Q_n)，其中$\frac{P_n}{Q_n}$是$\sqrt{d}$的第n个渐近分数．并且从证明过程可以看出，对于$\sqrt{d}$的任一渐近分数$\frac{P_n}{Q_n}$，都有

$$P_n^2-dQ_n^2=(-1)^nq_n$$

由于$l\neq(-1)^nq_n$且$|l|<\sqrt{d}$，所以要证明定理的后一部分，只需证明，当

$$|p^2-dq^2|<\sqrt{d}$$

时，$\frac{p}{q}$一定是$\sqrt{d}$的一个渐近分数就可以了．更一般地对于任一正实数α，$\alpha>1$。当

$$|p^2-\alpha^2q^2|<\alpha\ (p>0,\ q>0)$$

时，$\frac{p}{q}$是 α 的一个渐近分数就可以了

令 $\alpha^2q^2-p^2=\delta\theta\alpha$，$\delta=\pm1$，$0\leqslant\theta<1$，取 $\frac{p}{q}=[a_1, \cdots, a_n]=\frac{P^n}{Q^n}$，则

$$\alpha q-p=\frac{\delta\theta\alpha}{\alpha q+p} \tag{k}$$

$$\therefore\quad \varepsilon_n=\delta q(\alpha q-p)=\frac{\theta\alpha q}{\alpha q+p}=\frac{\theta\alpha Q_n}{\alpha Q_n+P_n},\quad \delta=(-1)^{n-1}$$

由(ii)知道，只需证明

$$\frac{\theta\alpha Q_n}{\alpha Q_n+P_n}<\frac{Q_n}{Q_n+Q_{n-1}}$$

或
$$\theta\alpha(Q_n+Q_{n-1})<\alpha Q_n+P_n \tag{l}$$

就可以了。当 $n=2$ 时，由于$0<\theta<1$，$Q_1=1$，而 $\theta\alpha Q_1=\theta\alpha<\alpha<\frac{P_2'}{Q_2}<p_2$，因而，有$\theta\alpha(Q_2+Q_1)<\alpha Q_2+P_2$

今若能证明

$$\alpha Q_n-P_n<\alpha(Q_n-Q_{n-1})\quad (n>2)$$

则问题便解决了。

由第一章第(5)式知，$Q_n=a_nQ_{n-1}+Q_{n-2}\geqslant Q_{n-1}+1$，且当$\alpha>1$时，$\alpha Q_n+P_n>1$，即

$$Q_n-Q_{n-1}\geqslant1>\frac{1}{\alpha Q_n+P_n}>\frac{\delta\theta}{\alpha Q_n+P_n} \tag{m}$$

然后在(m)的两边同乘以α，再由(k)即得

$$\alpha(Q_n-Q_{n-1})>\frac{\delta\theta\alpha}{\alpha Q_n+P_n}=\alpha Q_n-P_n$$

这就证明了定理的后一部分。

例9·3 $d=7$，$\alpha=\sqrt{d}=\sqrt{7}=[2,\dot{1},1,1,\dot{4}]$

a_s		2	1	1	1	4	1	1	1	4	…
P_s	1	2	3	5	8	37	45	82	127	635	…
Q_s	0	1	1	2	3	14	17	31	48	240	…

当 $n=3$时，$\alpha=\dfrac{\alpha_3P_3+P_2}{\alpha_3Q_3+Q_2}=\dfrac{5\alpha_3+2}{2\alpha_3+1}\Longrightarrow\alpha_3=\dfrac{\sqrt{7}+1}{3}$,

即$p_3=1$，$q_3=3$，故

$$x^2-7y^2=(-1)^33$$

有解 $x=5$，$y=2$。

若 $n=7$，$\alpha_7=\dfrac{P_6-\alpha Q_6}{\alpha Q_7-P_7}=\dfrac{45-17\sqrt{7}}{31\sqrt{7}-82}=\dfrac{\sqrt{7}+1}{3}$,

故 $x=82$，$y=31$是

$$x^2-7y^2=(-1)^73$$

的解。

定理9·13 设$\sqrt{d}=[a_1, a_2, \cdots, a_s, \dot{a}_{s+1}, \cdots, \dot{a}_{s+t}]$，若 $n>s$ 且

$$P_n^2-dQ_n^2=(-1)^nq_n$$

则

$$P_{n+lt}^2-dQ_{n+lt}^2=(-1)^{n+lt}q_n$$

证明 由于$\sqrt{d}$的循环节之长为 t，故

$$\alpha_n=\alpha_{n+lt}\Longrightarrow\frac{\sqrt{d}+p_n}{q_n}=\frac{\sqrt{d}+p_{n+lt}}{q_{n+lt}}$$

由定理9·12第一部分证明的过程可知，本定理是正确的。

下面将讨论著名的裴尔（Pell）方程

$$x^2-dy^2=\pm1 \tag{13}$$

由定理9·13知道，任给非平方的正整数 d，必有一个整

数q，使

$$x^2-dy^2=q \tag{14}$$

有无穷多个解．若把(14)的解(x_i, y_i)用mod|q|来分类，当$x_i \equiv x_j \pmod{|q|}$且$y_i \equiv y_j \pmod{|q|}$时，则称$(x_i, y_i)$与$(x_j, y_j)$属于同一类．记作

$$(x_i, y_i) \equiv (x_j, y_j) \pmod{|q|}$$

这样的类共有q^2个．所以必有一类其中至少有二解．即存在$x_1>0$，$y_1>0$；$x_2>0$，$y_2>0$，$x_1 \neq x_2$使得

$$x_1^2-dy_1^2=x_2^2-dy_2^2=q \text{ 且 } (x_1, y_1) \equiv (x_2, y_2) \pmod{|q|}$$

定理9·14 裴尔方程

$$x^2-dy^2=1 \tag{15}$$

有$y \neq 0$的解

$$x=\frac{x_1x_2-dy_1y_2}{q}, \quad y=\frac{x_1y_2-x_2y_1}{q} \tag{16}$$

其中$(x_1, y_1) \equiv (x_2, y_2) \pmod{|q|}$是(14)的两个解。

证明 (i) 先证(16)的x，y是整数．事实上

$$x_1x_2-dy_1y_2 \equiv x_1^2-dy_1^2=q \equiv 0 \pmod{|q|}$$

$$x_1y_2-x_2y_1 \equiv x_1y_1-x_1y_1=0 \pmod{|q|}$$

(ii) 次证$y \neq 0$。否则

$$x_1y_2-x_2y_1=0$$

由于$(x_1, y_1)=(x_2, y_2)=1$，因而$x_1=x_2$，$y_1=y_2$，这与$x_1 \neq x_2$的假设矛盾．

(iii) 最后证明(x，y)是(15)的解．事实上

$$q^2(x^2-dy^2)=(x_1x_2-dy_1y_2)^2-d(x_1y_2-x_2y_1)^2$$
$$=(x_1^2-dy_1^2)(x_2^2-dy_2^2)$$
$$=q^2$$
$$\therefore \quad x^2-dy^2=1$$

由定理9·12知道，(14)的解$\frac{x}{y}=\frac{P_n}{Q_n}$是$\sqrt{d}$的一个渐近分数，且存在n使得$(-1)^n q_n=1$，其中$q_n=\frac{\sqrt{d}+P_n}{\alpha_n}$。

定理9·15 设n是使$(-1)^n q_n=1$的最小正整数，用形式$x+y\sqrt{d}$来表示(15)的某一个解(x, y)，则这个解可由下式得到：

$$x+y\sqrt{d}=\pm(P_n+Q_n\sqrt{d})^l,\ l\gtreqless 0$$

证明 因为(P_n, Q_n)是(15)的一个解。用

$$\xi=P_n+Q_n\sqrt{d}$$

表示。显然$\xi>1$，且$\xi^l(l\gtreqless 0)$都是(15)的解。事实上，令$\bar{\xi}=P_n-Q_n\sqrt{d}$，则$\xi\bar{\xi}=P_n^2-dQ_n^2=1$，$\xi^l\bar{\xi}^l=(\xi\bar{\xi})^l=1^l=1$。

当$x+y\sqrt{d}$是(15)的一个解时，就有

$$\pm\frac{1}{x+y\sqrt{d}}=\pm(x-y\sqrt{d})$$

因而只需证明(15)的任一解$x+y\sqrt{d}$，$x>0$，$y>0$，都可以表成

$$x+y\sqrt{d}=\xi^m(m>0)$$

就可以了

设$x>0$，$y>0$，(x, y)是(15)的一个解，则

$$x+y\sqrt{d}>1$$

必存在一整数m，使得

$$\xi^m \leqslant x+y\sqrt{d}<\xi^{m+1}$$

即 $$1 \leqslant \xi^{-m}(x+y\sqrt{d})<\xi$$

令

$$\xi^{-m}(x+y\sqrt{d})=(x_0-y_0\sqrt{d})(x+y\sqrt{d})$$

$$=X+Y\sqrt{d} \qquad (\alpha)$$

因为$\sqrt{d}$是无理数，所以

$$(x_0+y_0\sqrt{d})(x-y\sqrt{d})=X-Y\sqrt{d} \qquad (\beta)$$

(α)，(β)的两边相乘得

$$X^2-dY^2=1$$

即(α)亦是(15)的一个解，今设

$$1<X+Y\sqrt{d}<\xi \Longrightarrow 0<\xi^{-1}<(X+Y\sqrt{d})^{-1}$$

$$=X-Y\sqrt{d}<1$$

$$\therefore \quad 2X=(X+Y\sqrt{d})+(X-Y\sqrt{d})>1+\xi^{-1}>0$$

$$2Y\sqrt{d}=(X+Y\sqrt{d})-(X-Y\sqrt{d})>1-1=0$$

因而得到

$$X^2-dY^2=1, \quad X>0, \quad Y>0$$

且由(α)及(α)的前一式得

$$1<X+Y\sqrt{d}<P_n+Q_n\sqrt{d}$$

因为$x=\sqrt{1+dy^2}$随$y(>0)$的增大而增大，故$x+y\sqrt{d}$亦随y的增大而增大。因而从上不等式可得$Y<Q_n$且$X<P_n$，而$\frac{X}{Y}$是一个分母小于Q_n的$\sqrt{d}$的渐近分数。这与n的最小性矛盾，故这是不可能的，所以只能$X^2+Y^2\sqrt{d}=1$，即$X=1$，$Y=0$。

由定理9·15知道$x^2-dy^2=1$都有解，并且$P_n+Q_n\sqrt{d}$

是它的最小解。但

$$x^2-dy^2=-1 \tag{17}$$

就不一定有解了。例如，$x^2-3y^2=-1$无解，因为 $x^2\equiv 0$，$1 \pmod 4$，而 $x^2-3y^2\equiv x^2+y^2\equiv 0$，$1$，$2 \pmod 4$，而$\not\equiv -1 \pmod 4$，故无解。这个例子说明，一切 $d\equiv 3 \pmod 4$ 时(17)无解。

系 1　若(17)有解(x_0, y_0)则由

$$x_1+y_1\sqrt{d}=(x_0+y_0\sqrt{d})^2$$

所确定的(x_1, y_1)是(15)的解。

系 2　若(17)有解，则

$$x^2-dy^2=\pm 1$$

的一切解可由

$$\pm(P_n+Q_n\sqrt{d})^t$$

给出，其中 n 是使$(-1)^n q_n=-1$成立的最小正整数。

系的证明留给读者完成。

第四节　一般二次不定方程

一般的二次不定方程

$$ax^2+bxy+cy^2+dx+ey+f=0 \tag{18}$$

令 $D=b^2-4ac$，若$D=0$，则以$4a$乘(18)式得

$$(2ax+by)^2+4adx+4aey+4af=0$$

此类不定方程的解法也比较容易。我们令$2ax+by=t$，则上式变为

$$t^2+2dt+2(2ae-bd)y+4af=0$$

$$(t-d)^2=2(bd-2ae)y+d^2-4af$$

先由同余式

$$(t+d)^2\equiv d^2-4af(\bmod 2(bd-2ae))$$

求 t，次求 y，x 就得到(18)的整数解。

若D≠0，以D^2乘(18)式，得

$$aD^2x^2+bD^2xy+cD^2y^2+dD^2x+eD^2F+fD^2=0 \quad (19)$$

令

$$Dx=x'+2cd-bc,\quad Dy=y'+2ae-bd$$

代入(19)得

$$a(x'+2cd-be)^2+b(x'+2cd-be)(y'+2ae-bd)$$
$$+(y'+2ae-bd)^2+dD(x'+2cd-be)$$
$$+eD(y'+2ae-bd)+fD^2=0.$$

即 $$ax'^2+bx'y'+cy'^2=k \quad (19')$$

其中

$$k=a(be-2cd)^2+b(be-2cd)(bd-2ae)$$
$$+c(bd-2ae)^2+dD(be-2cd)+eD(bd-2ae)$$
$$+fD^2\equiv a(be-2cd)^2+b(be-2cd)(bd-2ae)$$
$$+c(bd-2ae)^2(\bmod |D|)$$

所以(18)是否有解，依赖于(19′)能否适合

$$x'\equiv be-2cd,\quad y'\equiv bd-2ae\ (\bmod |D|) \quad (20)$$

的解答．换言之，求一般的二元二次同余式(18)的解的问题，转化为能否求出适合条件(20)的(19′)的解的问题．因此归结为求形如(19′)的方程的解问题。

定义9·4 整系数二次不定方程

$$ax^2+bxy+cy^2=k \quad (19'')$$

中 $d=b^2-4ac$（注意，这里的 d 不是(18)中 x 的系数 d）是一个非平方数，$(a,b,c)=1$，若有$(x,y)=1$的解时，这个解叫做(19′)的既约解（proper solution）或正常解。

(19′)中的 k 若是负数，则可把 a，b，c 改变符号，使右边的常数项为正，而不改变 d 的值及 a，b，c 的互素

性。故下面假设k是正的。

定理9·16 若x，y是一个既约解，则可以唯一定出二整数s及r，使

$$xs-yr=1 \tag{21}$$

及
$$l=(2ax+by)r+(bx+2cy)s \tag{α}$$

适合

$$l^2\equiv d\ (\mathrm{mod}\ 4k),\quad 0\leqslant l<2k \tag{22}$$

证明 由定理1·12知，(21)有解r_0，s_0，且其一般解是

$$r=r_0+hx,\quad s=s_0+hy\ (h=0,\ \pm1,\ \pm2,\ \cdots)$$

于是

$$\begin{aligned}l&=(2ax+by)r_0+(bx+2cy)s_0+2h(ax^2+bxy+cy^2)\\&=l_0+2hk\end{aligned}$$

由于有唯一的整数h适合$-\frac{l_0}{2k}\leqslant h<1-\frac{l_0}{2k}$，故有唯一的$h$适合$0\leqslant l<2k$。又

$$\begin{aligned}l^2&=[(2ax+by)r+(bx+2cy)s]^2\\&=4(ar^2+brs+cs^2)(ax^2+bxy+cy^2)\\&\quad+(b^2-4ac)(xs-yr)^2\\&=4k(ar^2+brs+cs^2)+d\equiv d\ (\mathrm{mod}\ 4k)\end{aligned}$$

定理9·17 若$(x_1,\ y_1)$与$(x_2,\ y_2)$是(19″)的对应于同一的l的两个既约解，则它们之间有下列的关系：

$$\begin{aligned}&2ax_1+(b+\sqrt{d})y_1\\&\quad=[2ax_2+(b+\sqrt{d})y_2]\left(\frac{t+u\sqrt{d}}{2}\right)\end{aligned} \tag{23}$$

其中t及u为

$$t^2-du^2=4 \tag{24}$$

的整数解。反之，若$(x_2,\ y_2)$是(19″)的一个既约解，则由(23)所确定的$(x_1,\ y_1)$也是(19″)的一个既约解，且有相同的l。

定理9·16指出了，(19″)的每一个既约解都对应于一个满足条件(22)的 l，并且这样的 l 是唯一的。但是是否不同的既约解，都对应于不同的 l 呢？答案是否定的。定理9·17就给出了，对应于同一 l 的两个既约解之间的关系。并且指出具有关系(22)的两组数 (x_1, y_1)，(x_2, y_2) 之一是(19″)的既约解时，则另一个也是(19″)的既约解。先证

引理 1 (24)有解

$$\begin{cases} t = [(2ax_1+by_1)(2ax_2+by_2)-dy_1y_2]/2ak \\ u = -(x_1y_2-x_2y_1)/k \end{cases} \tag{25}$$

其中 (x_1, y_1)，(x_2, y_2) 是(19″)的两个同对应于 l 的既约解，并且 (x_1, y_1)，(x_2, y_2)，(t, u) 满足(23)。

证明 (i) 先证(25)满足(24)且有等式(23)。因为

$$\frac{t^2-du^2}{4} = \frac{t-\sqrt{d}u}{2} \cdot \frac{t+\sqrt{d}u}{2}$$

$$= \frac{(2ax_1+by_1)(2ax_2+by_2)-dy_1y_2+2a(x_1y_2-x_2y_1)\sqrt{d}}{4ak}$$

$$\cdot \frac{(2ax_1+by_1)(2ax_2+by_2)-dy_1y_2-2a(x_1y_2-x_2y_1)\sqrt{d}}{4ak}$$

$$= \frac{(2ax_1+by_1-\sqrt{d}y_1)(2ax_2+by_2+\sqrt{d}y_2)}{(2ax_1+by_1+\sqrt{d}y_1)(2ax_1+by_1-\sqrt{d}y_1)}$$

$$\cdot \frac{(2ax_1+by_1+\sqrt{d}y_1)(2ax_2+by_2-\sqrt{d}y_2)}{(2ax_2+by_2-\sqrt{d}y_2)(2ax_2+by_2-\sqrt{d}y_2)} = 1$$

故(25)满足(24)。然后用

$$\frac{(2ax_1+by_1+\sqrt{d}\,y_1)(2ax_2+by_2-\sqrt{d}\,y_2)}{(2ax_2+by_2-\sqrt{d}\,y_2)(2ax_2+by_2+\sqrt{d}\,y_2)}$$ 代(23)中的 $\frac{t+u\sqrt{d}}{2}$，就使等式成立。事实上，上式的分子是用视察法（十字乘法）分解因式，分母

$$\begin{aligned}4ak &= 4a^2x_1^2+4abx_1y_1+4acy_1^2\\ &=(2ax_1+by_1)^2-(\sqrt{d}\,y_1)^2\\ &=(2ax_1+by_1+\sqrt{d}\,y_1)(2ax_1+by_1-\sqrt{d}\,y_1)\end{aligned}$$

(ii) 次证(25)中的 t，u 是整数。由(α)

$$\begin{aligned}2ax_1+by_1 &= (2ax_1+by_1)(s_1x_1-r_1y_1)\\ &=(2ax_1+by_1)s_1x_1-ly_1+(bx_1+\\ &\quad +2cy_1)s_1y_1\\ &=2ks_1-ly_1\equiv -ly_1 \pmod{2k} \qquad (\beta)\end{aligned}$$

由于(x_2, y_2)亦是(19″)对应于 l 的既约解，故得

$$2ax_2+by_2\equiv -ly_2 \pmod{2k} \qquad (\gamma)$$

$y_2(\beta)+y_1(\gamma)$得

$$2a(x_1y_2-x_2y_1)\equiv 0 \pmod{2k}$$

$x_2(\beta)+x_1(\gamma)$得

$$(b+l)(x_1y_2-x_2y_1)\equiv 0 \pmod{2k}$$

在(19″)中 c 与 a 是“对称”的（意即互换 x，y，a，c 的结果相同）故同法可得

$$2c(x_1y_2-x_2y_1)\equiv 0 \pmod{2k}$$

$$(b-l)(x_1y_2-x_2y_1)\equiv 0 \pmod{2k}$$

但

$$(2a,\ b+l,\ 2c,\ b-l)=(2a,\ 2b,\ 2c,\ b+l)\leqslant 2$$

$$\therefore \qquad x_1y_2-x_2y_1\equiv 0 \pmod{k}$$

即 u 是整数。由(24)知 $t^2=4+du^2$ 亦是整数，(25)中的 t 是有理数，其平方是整数，故 t 亦是整数。

引理 2 具有条件(23)、(24)的(19″)的两个解 $(x_1, y_1)(x_2, y_2)$，必有如下的关系：

$$\begin{cases} x_1 = \dfrac{t-bu}{2}x_2 - cuy_2 \\ y_1 = aux_2 + \dfrac{t+bu}{2}y_2 \end{cases} \tag{26}$$

且若 (x_1, y_1) 是(19″)的既约解，(r_1, s_1) 对应于 (x_1, y_1) 时，则有关系

$$r_2 = \frac{t+bu}{2}r_1 + cus_1,\quad s_2 = -aur_1 + \frac{t-bu}{2}s_1 \tag{27}$$

的 (r_2, s_2) 对应于 (x_2, y_2)，并且 (x_2, y_2) 亦是(19″)的既约解。

证明 设 $t^2-du^2=4$ 且

$$2ax_1+(b+\sqrt{d})y_1 = [2ax_2++(b+\sqrt{d})y_2]$$

$$\left(\frac{t+u\sqrt{d}}{2}\right) \Longrightarrow (2ax_1+by_1)+y_1\sqrt{d}$$

$$=\left(atx_2+\frac{bt+du}{2}y_2\right)+\left(aux_2+\frac{bu+t}{2}y_2\right)\sqrt{d}$$

$$\Longrightarrow 2ax_1+by_1 = atx_2+\frac{bt+du}{2}y_2, y_1 = aux_2+\frac{bu+t}{2}y_2$$

$$\Longrightarrow \begin{cases} x_1 = \dfrac{t-bu}{2}x_2 - cuy_2 \\ y_1 = aux_2 + \dfrac{t+bu}{2}y_2 \end{cases}$$

由于 t，u 是适合(24)的二整数，若 (r_1, s_1) 对应于 (x_1, y_1)，即 $x_1s_1-y_1r_1=1$，且

$$r_2=\frac{t+bu}{2}r_1+cus_1,\quad s_2=-aur_1+\frac{t-bu}{2}s_1$$

则(r_2, s_2)对应于(x_2, y_2)，且$(x_2, y_2)=1$。事实上

$$1=x_1s_1-y_1r_1=\left(\frac{t-bu}{2}x_2-cuy_2\right)s_1$$

$$-\left(aux_2+\frac{t+bu}{2}y_2\right)r_1$$

$$=x_2\left(\frac{t-bu}{2}s_1-aur_1\right)-y_2\left(cus_1+\frac{t+bu}{2}r_1\right)$$

$$=x_2s_2-y_2r_2$$

有了引理1与引理2，要证明定理9·17只需证明适合条件(23)的(19″)的两个既约解，它们所对应的l_1，l_2必相等。

定理的证明：设l_1，l_2分别对应于(19″)的两个既约解(x_1, y_1)，(x_2, y_2)，则

$$l_1=2ax_1r_1+b(x_1s_1+y_1r_1)+2cy_1s_1$$

$$=(2ar_1+bs_1)\left(\frac{t-bu}{2}x_2-cuy_2\right)+$$

$$+(br_1+2cs_1)\left(aux_2+\frac{t+bu}{2}y_2\right)$$

$$=\left[2a\left(r_1\frac{t-bu}{2}+s_1cu\right)\right.$$

$$\left.+b\left(s_1\frac{t-bu}{2}+r_1au\right)\right]x_2$$

$$+\left[b\left(r_1\frac{t+bu}{2}-s_1cu\right)\right.$$

$$\left.+2c\left(s_1\frac{t+bu}{2}-r_1au\right)\right]y_2$$

$$=2ax_2r_2+b(x_2s_2+y_2r_2)+2cy_2s_2$$

$$=l_2$$

下面分 $d>0$ 及 $d<0$ 两种情况来讨论。

定理9·18 设 $d<0$。令

$$w=\begin{cases}2, & 若\ d<-4\\ 4, & 若\ d=-4\\ 6, & 若\ d=-3\end{cases}$$

则(19″)有 w 个既约解，对应于同一 1。

证明 由定理9·17知，我们只需证明，对于任给的 d，方程

$$t^2-du^2=4 \tag{24}$$

的解数是 w 就可以了。

若 $d<-4$，显然(24)有且只有 $t=\pm2$，$u=0$两个解，即 $w=2$。

若 $d=-4$，则

$$t^2+4u^2=4$$

有且只有 $t=\pm2$，$u=0$；$t=0$，$u=\pm1$ 四个解，即 $w=4$。

若 $d=-3$，则

$$t^2+3u^2=4$$

有且只有 $t=\pm2$，$u=0$；$t=\pm1$，$u=\pm1$六个解。即 $w=6$。

定理9·19 若 $d>0$，则(24)的诸解，可由下面的方法得到。

设(x_0, y_0)是(24)的诸解中使 $x_0+y_0\sqrt{d}$ $(x_0>0, y_0>0)$为最小的一个解，则(24)的一切解(x, y)，可由

$$\frac{x+y\sqrt{d}}{2}=\pm\left(\frac{x_0+y_0\sqrt{d}}{2}\right)^n,$$

得出，其中 n 是任意整数。

这定理的证法与定理9·15一致，因为 $x^2-dy^2=1$ 必有最小解 $x_1+y_1\sqrt{d}$，则 $2x_1+2y_1\sqrt{d}=x_0+y_0\sqrt{d}$ 是

(24)的解。令

$$\xi=\frac{x_0+y_0\sqrt{d}}{2},\quad \overline{\xi}=\frac{x_0-y_0\sqrt{d}}{2}$$

因为$\frac{x_0}{2}=x_1$，$\frac{y_0}{2}=y_1$是整数，故(24)可转化为$x^2-dy^2=1$的问题。所以下面的证法完全与定理9·15一致。

这个定理更一般的形式是

系 若$d>0$，则

$$x^2-dy^2=h^2$$

都有解。若其最小解是$x_0+y_0\sqrt{d}$，则所有解可由

$$\frac{x+y\sqrt{d}}{h}=\pm\left(\frac{x_0+y_0\sqrt{d}}{h}\right)^n \quad n \gtrless 0$$

得出。

定义9·5 设$d>0$，$\xi=\frac{x_0+y_0\sqrt{d}}{2}$，(19″)式适合于

$$2ax+(b-\sqrt{d})y>0,\quad 1\leqslant\left|\frac{2ax+(b+\sqrt{d})y}{2ax+(b-\sqrt{d})y}\right|<\xi^2 \quad (28)$$

的解，称为(19″)的原解(primary solution)。

若令

$$L=2ax+(b+\sqrt{d})y,\quad \overline{L}=2ax+(b-\sqrt{d})y$$

则条件(28)变为

$$\overline{L}>0,\quad 1\leqslant\left|\frac{L}{\overline{L}}\right|<\xi^2 \quad (28')$$

定理9·20 若$d>0$，(19″)有对应于某一l的既约解，对应于同一l的既约原解是唯一的。这里的l是定理9·16中所定义的。

证明 由定理9·17、9·19知道，若(x_0, y_0)是(19″)的一个既约原解。设L_0是它所对应的L，即

$$L_0 = 2ax_0 + (b+\sqrt{d})y_0.$$

则凡是(19″)式中对应于同一l的既约解$x+\sqrt{d}y$所对应的L可表为

$$L = \pm L_0\xi^n$$

即

$$2ax + (b+\sqrt{d})y$$

$$= \pm[2ax_0 + (b+\sqrt{d})y_0]\left(\frac{x_0 + y_0\sqrt{d}}{2}\right)^n$$

的形式。已知

$$\left|\frac{L}{\bar{L}}\right| = \left|\frac{L_0\xi^n}{\bar{L}_0\bar{\xi}^n}\right| = \left|\frac{L_0}{\bar{L}_0}\right|\xi^{2n}$$

只有当$n=0$时，

$$1 \leqslant \left|\frac{L}{\bar{L}}\right| = \left|\frac{L_0}{\bar{L}_0}\right| < \xi^2, \quad \bar{L} = \bar{L}_0 > 0$$

定理得证，事实上，若$n>0$，则

$$1 < \xi^{2n} \leqslant \left|\frac{L}{\bar{L}}\right| = \left|\frac{L_0}{\bar{L}_0}\right|\xi^{2n} < \xi^{2n+2}$$

对应这样L的解$x+y\sqrt{d}$就不是原解了。

若$d>0$命$w=1$，结合定理9·18中的w值，可把定义9·5推广于下：

定义9·5′ 当$d>0$时，原解的定义如定义9·5；若$d<0$时，把(19″)的一切既约解，都叫做它的原解。

于是定理9·18和9·20可合并为

定理9·21 对应于同一l，(19)″若有既约原解，则只有w个既约原解。

定理9·20给我们指出了，要求双曲线

$$ax^2+bxy+cy^2=k \tag{19''}$$

上的整点（求其整数解）时，不必在整条双曲线上探索。原解仅在一有限的双曲线上，得到原解后，可由公式 $L=\pm L_0\xi^n$ 得出(19″)的一切既约解。即若 ξ 已知，仅须经有限步骤就可以获得(19″)的所有的解。更确切地说，从

$$L_0\overline{L_0}=4ak,\ \overline{L_0}>0,\ 1\leqslant\left|\frac{L_0}{\overline{L_0}}\right|<\xi^2$$

可知

$$|\overline{L_0}|\leqslant|L_0|=\sqrt{\left|\frac{L_0\overline{L_0}}{\overline{L_0}}\right|^2}=2\sqrt{|ak|}\sqrt{\left|\frac{L_0}{\overline{L_0}}\right|}<2\sqrt{|ak|}\xi$$

即

$$|2\sqrt{d}\,y|=|L_0-\overline{L^0}|\leqslant|L_0|+|\overline{L_0}|<4\sqrt{|ak|}\,\xi$$

$$\therefore\qquad |y|\leqslant 2\xi\sqrt{\frac{|ak|}{d}} \tag{29}$$

故只须找出(19″)的解就可以了，其余诸解可由公式 $L=\pm L_0\xi^n$ 得出

$$0<2\sqrt{d}\,y=L-\overline{L}\leqslant L=\sqrt{L\overline{L}\frac{L}{\overline{L}}}\leqslant\varepsilon\sqrt{4ak}$$

$$\therefore\qquad 0<y\leqslant\xi\sqrt{\frac{ak}{d}}$$

此结果在计算中比(29)的界限略佳。

下面介绍(19″)的求解方法，今就 $d>0$ 非平方数的情况进行讨论，(19″)可改写为

$$(2ax+by)^2-dy^2=4ak$$

因此要解这个方程，首先要解决

$$x^2-dy^2=\delta k,\ k>0,\ \delta=\pm1 \tag{30}$$

的求解问题。

由定理9·12知道 $k<\sqrt{d}$ 时，(30)的解是$\sqrt{d}$的渐近分数，其循环节之长为 t 时，若(P_n, Q_n)是(30)之解，则(P_{n+st}, Q_{n+st})也是(30)的解。因此经过有限次的试根可得(30)的一切解。

下面将把 $k>\sqrt{d}$ 的情况转化为 $k<\sqrt{d}$ 的情况，使得容易用定理9·12的方法，讨论其解的存在与解法。

设 $k>\sqrt{d}$，且(x，y)是(30)的既约解。则 x_1及 y_1 使

$$xy_1-yx_1=\delta \tag{31}$$

以$x_1^2-dy_1^2$乘(30)的两边，得

$$(xx_1-dyy_1)^2-d(xy_1-x_1y)^2=\delta k(x_1^2-dy_1^2)$$

即

$$(xx_1-dyy_1)^2-d=\delta k(x_1^2-dy_1^2) \tag{32}$$

设(x_0, y_0)是(31)的一个解，则(31)的一切解是

$$x_1=x_0+tx,\quad y_1=y_0+ty$$

$$\begin{aligned}\therefore\quad xx_1-dyy_1&=xx_0-dyy_0+(x^2-dy^2)t\\&=xx_0-dyy_0+\delta tk\end{aligned}$$

故可取适当的 t 值使

$$|xx_1-dyy_1|\leqslant\frac{k}{2}$$

事实上，若由带余除法得$-xx_0+dyy_0=kq+r$，$|r|\leqslant\frac{k}{2}$，则当$\delta=1$时，取$t=q$；当$\delta=-1$时，取$t=-q$。

令$|xx_1-dyy_1|=l$，由(32)、(31)即得

$$x_1^2 - dy_1^2 = \frac{l^2 - d^2}{\delta k} = \eta_1 h_1,\ \eta_1 = \pm 1,\ h_1 > 0 \quad (30')$$

又因 $k^2 > d$，$l^2 \leqslant \frac{k^2}{4} < k^2$，故

$$h_1 \leqslant \frac{\max(d,\ l^2)}{k} < \frac{k^2}{k} = k.$$

由此可见，当 $k > \sqrt{d}$ 时，(30)的一解(x, y)可以得出形式一样的 $h_1 < k$ 的方程(30′)的一解(x_1, y_1)。若 $h_1 > \sqrt{d}$，则可继续使用上法，达到 h 小于$\sqrt{d}$的情况出现为止。由上面的 l 的定义又可知

$$\begin{aligned} l^2 &\equiv (xx_0 - dyy_0)^2 = x^2x_0^2 - 2dxx_0yy_0 + d^2y^2y_0^2 \\ &\equiv x^2x_0^2 - 2dxx_0yy_0 + d^2y^2y_0^2 - x^2x_0^2 + dx_0^2y^2 \\ &\quad + dx^2y_0^2 - d^2y^2y_0^2 \equiv dx_0y(x_0y - xy_0) \\ &\quad - dxy_0(x_0y - xy_0) = d(x_0y - xy_0)^2 = d\delta^2 \\ &\equiv d(\mathrm{mod}\ k) \end{aligned}$$

且$0 \leqslant l \leqslant \frac{k}{2}$。这样，根据上面的讨论，可得下面求解的方法。

先求适合下面条件的 l 和 h_1（有时 h_1 不是唯一的）：

$$l^2 \equiv d\ (\mathrm{mod}\ k),\ 0 \leqslant l \leqslant \frac{k}{2},$$

$$\frac{l^2 - d}{\delta k} = \eta h,\ \eta = \pm 1,\ h_1 > 0.$$

把方程(30)转化为(30′)，若 $h_1 > \sqrt{d}$，则继续上法，求出适合下面条件的 $l_1, l_2, \cdots, l_t$ 及 $h_1, h_2, \cdots, h_t$：

$$l_i^2 \equiv d(\mathrm{mod}\ h_i),\ 0 \leqslant l_i \leqslant \frac{h_i}{2},\ l_i^2 = d + h_ih_{i+1}$$

令 $\dfrac{l_i^2-d}{\eta_i h_i}=\eta_{i+1}h_{i+1}$，$\eta_s=\pm 1$，$h_s>0$（当 $s=0$ 时，$\eta_0=\delta$，$h_0=k$）。依相反的次序解下面诸方程

$$\begin{aligned}&x^2-dy^2=\delta k,\\&x_1^2-dy_1^2=\eta_1 h_1,\\&\cdots\cdots,\\&x_t^2-dy_t^2=\eta_t h_t.\ h_t<\sqrt{d}\end{aligned}\tag{30''}$$

其方法是：用连分数解(30″)的最后一个方程，若 (x_t, y_t) 是它的一个解，则

$$x_{t-1}=\frac{-\eta_{t-1}dy_t\pm l_{t-1}x_t}{\eta_t h_t},\quad y_{t-1}=\frac{-\eta_{t-1}x_t\pm l_{t-1}y_t}{\eta_t h_t}\tag{33}$$

当它是整数时，便是(30″)倒数第二个方程的解，依此类推，可求(30″)第一个方程的解，事实上，因为

$$\begin{aligned}x_{t-1}^2-dy_{t-1}^2&=\left(\frac{-\eta_{t-1}dy_t\pm l_{t-1}x_t}{\eta_t h_t}\right)^2\\&\quad-d\left(\frac{-\eta_{t-1}x_t\pm l_{t-1}y_t}{\eta_t h_t}\right)^2\\&=\frac{\left(l_{t-1}^2-d\right)\left(x_t^2-dy_t^2\right)}{h_t^2}\\&=\frac{l_{t-1}^2-d}{\eta_t h_t}\\&=\eta_{t-1}h_{t-1}.\end{aligned}$$

依此类推，可求出(30″)第一式的解。

例9·4 解不定方程

$$x^2-15y^2=61.\tag{α}$$

解 先求适合

$$l^2 \equiv 15 \pmod{61}, \quad 0 \leqslant l \leqslant \frac{61}{2}$$

的诸解，也就是在

$$l^2 = 15 + 61h, \quad l^2 \leqslant 900 \tag{β}$$

中，求适当的 h，使$15+61h$是一个平方数．令 h 经过 $0 \leqslant h \leqslant \left[\frac{900}{61}\right] = 14$，逐一代入(β)可知有且只有 $h=10$ 时，$l^2 = 625 = 25^2$，即

$$l = 25, \quad h = 10, \quad \eta = 1$$

故解方程(α)转化为解方程

$$x_1^2 - 15y_1^2 = 10 \tag{γ}$$

但$10 > \sqrt{15}$，故再求

$$l_1^2 = 15 + 10h_1, \quad 0 \leqslant l_1 \leqslant \frac{10}{2} = 5$$

的诸解．当且仅当 $l_1 = 5$，$h_1 = 1$，$\eta_1 h_1 = \frac{25-15}{10} = 1$．故转化为求解方程

$$x_2^2 - 15y_2^2 = 1 \tag{δ}$$

由连分数法，知(δ)的解答是

$$x_2 + y_2\sqrt{15} = \pm(4+\sqrt{15})^n$$

由公式(33)得

$$x_1 = \frac{-15 \pm 5 \times 4}{1} = 5, \; -35, \quad y_1 = \frac{-4 \pm 5 \times 1}{1} = 1, -9$$

取$(x_1, y_1) = (5, 1)$，则(γ)的解是

$$x_1 + y_1\sqrt{15} = \pm(4+\sqrt{15})^n(5 \pm \sqrt{15})$$

因而(α)的解是

$$x + y\sqrt{15} = \pm(4+\sqrt{15})^n(5 \pm \sqrt{15})(25 \pm \sqrt{15})/10$$

其中正负号可以任意选取。故得

$$x+y\sqrt{15}=\pm(4+\sqrt{15})^n(14\pm3\sqrt{15})$$

$$\text{或}\quad =\pm(4+\sqrt{15})^n(11\pm2\sqrt{15})$$

另一种解法。由不等式(29)，得

$$0<y\leqslant\xi\sqrt{\frac{ak}{d}}\Longrightarrow0<y\leqslant7$$

事实上，因为 $x^2-15y^2=4$ 的最小解是 $8+2\sqrt{15}$，

$\xi=\dfrac{8+2\sqrt{15}}{2}$，(α)中 $a=1, b=0, c=-15, d=b^2-4ac=60$

$k=61$，故 $\xi\sqrt{\dfrac{ak}{d}}\doteq7.9<8$。其解法可列表于下：

y	1	2	3	4	5	6	7
$15(2y-1)$	15	45	75	105	135	165	195
$15y^2$	15	60	135	240	375	540	735
$15y^2+61$	76	121	196	301	436	601	796

注意：上表的计算方法如下：第二行的每一项都是前一项加30，第三行的第 i 项是第 i－1项加上第二行的第 i 项得到的；第四行是由第三行加上61而得到。当表的第四行出现完全平方数时，就得到(α)的一个整数解。如(11，2)，(14，3)等。

第五节　二次型上的整点

定义9·6　若(a，b，c)＝1，则称二次型

$$F=F(x,\ y)=ax^2+bxy+cy^2$$

为原型（primary form）。若(a，b，c)＝g>1，则称{a，b，c}为非原型（im-primary form）。

显然$\left\{\frac{a}{g}, \frac{b}{g}, \frac{c}{g}\right\}$是原型。若$\{a,b,c\}$的判别式为d，则$\left\{\frac{a}{g}, \frac{b}{g}, \frac{c}{g}\right\}$的判别式为$\frac{d}{g^2}$。由定理9·2知道，若$\{a,b,c\}\sim\{a_1, b_1, c_1\}$则它们同为原型或同为非原型。

用h(d)代表以d为判别式的原型的类数（$d<0$时表示定正型的类数）。例如

$h(-4)=1$，即$\{1, 0, 1\}$为代表的一个类；

$h(-20)=2$，即$\{1, 0, 5\}$，$\{2, 2, 3\}$为代表的两个类；而$h\left(\frac{d}{g^2}\right)=h\left(\frac{-20}{4}\right)=h(-5)=0$等等。

由定理9·5知，$0<a\leqslant\sqrt{\frac{|d|}{3}}$，当$d=-80$时，$0<a\leqslant5$，由定理9·6知，符合$d=-80$的已化型有$\{1, 0, 20\}$，$\{2, 0, 10\}$，$\{3, 2, 7\}$，$\{4, 0, 5\}$，$\{4, 4, 6\}$等五个定正型的类，其中$\{2, 0, 10\}$，$\{4, 4, 6\}$不是原型。故$h(-80)=3$，$h\left(\frac{-80}{4}\right)=h(-20)=2$，$h\left(\frac{-80}{16}\right)=h(-5)=0$。故以$d=-80$为判别式的型的类数等于：

$h(-80)+h(-20)+h(-5)=3+2+0=5$

一般地，以d为判别式的型的类数等于

$$\sum_{\substack{g^2\mid d\\ g>0}} h\left(\frac{d}{g^2}\right) \tag{34}$$

于诸原型类中每类取一代表（若是定型，则讨论诸原定正型类），而得一代表团，记作

$$F_1, F_2, \cdots, F_{h(d)}. \tag{35}$$

定理9·22 设$h>0$，$(k, d)=1$，令$\psi(k)$表示诸二元二次型

$$k=F_1(x,y),k=F_2(x,y),\cdots,k=F_{k(d)}(x,y) \qquad (36)$$

的原解（定义9·5′）的个数的总和，则

$$\psi(k)=w\sum_{n\mid k}\left(\frac{d}{n}\right) \qquad (37)$$

其中 w 的定义如定理9·18及 $d>0$时，$w=1$，$\left(\frac{d}{n}\right)$是克朗里克符号。

证明 由定理9·21知，(36)的每一个方程中对应于同一 l 的既约原解的个数等于 w．若 l 是同余式

$$l^2\equiv d(\bmod 4k) \quad 0\leqslant l<2k \qquad (11'')$$

的解，则可由 $l^2-4km=d$ 定出一整数 m，从而得到一型 $\{k, l, m\}$，它是判别式为 d 的原型。事实上，若 $(k,l,m)=g>1$，则 $g\mid k$，$g\mid d$，这与 $(k, l)=1$ 的假设矛盾．故 $\{k, l, m\}$ 必与(35)中一个F相似，且只与其中之一相似。由定理9·21知道，这样的 F_i 对应于这个 l 的既约原解有ω个又由定理9·10的系知道，$(11'')$的解 l 共有 $\sum_{f\mid k}\left(\frac{d}{f}\right)$个。故(36)的既约解的总数是

$$w\sum_{f\mid k}\left(\frac{d}{f}\right)$$

又诸原解的总数为

$$\psi(k)=w\sum_{\substack{g^2\mid k\\ g>0}}\ \sum_{f\mid \frac{k}{g^2}}\left(\frac{d}{f}\right)$$

$\left(因(k, d)=1，故\left(\frac{k}{g^2}, d\right)=1\right)$。因$(g^2, d)=1$，故

$$\psi(k)=w\sum_{\substack{g^2\mid k\\ g>0}}\ \sum_{f\mid \frac{k}{g^2}}\left(\frac{d}{fg^2}\right)=w\sum_{n\mid k}\left(\frac{d}{n}\right)$$

事实上，任一整数 n 必可表成 $n=fg^2$，f 无平方因子且 $g>0$。又 $g^2|k$，$f\left|\frac{k}{g^2}\right.\Longleftrightarrow n|k$

例如，由于 $h(-4)=1$，故 $\psi(k)$ 即为 $x^2+y^2=k$，$(k, d)=1$ 的解数 $r(k)$（第八章第二节五），由定理9·18知，$d=-4$ 时，$w=4$，而

$$\left(\frac{d}{n}\right)=\begin{cases}1, & 若\ n\equiv 1 \pmod 4\\ -1, & 若\ n\equiv 3 \pmod 4\end{cases}$$

故有与第八章第二节五中同样的结论：

定理9·23 不定方程

$$x^2+y^2=k \tag{38}$$

的解数

$$\psi(k)=4(\tau_1(k)-\tau_3(k))$$

其中 $\tau_1(k)$，$\tau_3(k)$ 分别是 k 的 $4m+1$ 形和 $4m+3$ 形的正因数的个数。

这个定理给出了圆周(38)上的整点的个数。如，$k=5$，$r(5)=\psi(5)=8$，即圆周 $x^2+y^2=5$ 上有八个整点 $(\pm 1, \pm 2)$，$(\pm 2, \pm 1)$；$k=35$ 时，$r(35)=\psi(35)=4\times(2-2)=0$；$\psi(13\times 7\times 11)=4(4-4)=0$；$\psi(13\times 5\times 7)=4(4-4)=0$；$\psi(13\times 5\times 7^2)=4\times(8-4)=16$ 等等。或用第八章等式(35)来计算如，$\psi(13\times 5\times 7^2)=4\times(1+1)\times(1+1)\times\times\left(\frac{1+(-1)^2}{2}\right)=16$；$\psi(13\times 5\times 7)=4\times(1+1)\times(1+1)\times\frac{(1-1)}{2}=0$。

若 $k=2^{\alpha}N$，由第八章第二节五知道

$\delta(k)=\delta(N)$，$r(k)=4\delta(k)=4\delta(N)$

所以定理9·23对于 k 包含 2^{α} 的因数的情况，其结论仍然成

立．如，$\psi(10)=\psi(5)=8$，即圆周 $x^2+y^2=10$上有八个整点 $(\pm1,\ \pm3)$，$(\pm3,\ \pm1)$；$\psi(20)=\psi(5)=8$，$(\pm2,\ \pm4)$ 和$(\pm4,\ \pm2)$是 $x^2+y^2=20$上的八个整点等等。

下面将讨论圆(38)内的整点问题．为此先证

定理9·24 （Abel定理）设 $a\leqslant b$，变数 n 在 $a\leqslant n\leqslant b$ 中变化，γ_n，ε_n是复数，令

$$s_n=\sum_{a\leqslant m\leqslant n}\gamma_m,$$

则

$$\left|\sum_{n=a}^{b}\gamma_n\varepsilon_n\right|\leqslant\max_{a\leqslant n\leqslant b}|s_n|\left(\sum_{a\leqslant m\leqslant b-1}|\varepsilon_m-\varepsilon_{m+1}|+|\varepsilon_b|\right)\quad(39)$$

证明 令 $s_{a-1}=0$，则

$$\begin{aligned}\sum_{n=a}^{b}\gamma_n\varepsilon_n&=\sum_{n=a}^{b}(s_n-s_{n-1})\varepsilon_n\\&=\sum_{n=a}^{b}s_n\varepsilon_n-\sum_{n=a}^{b-1}s_n\varepsilon_{n+1}\\&=\sum_{n=a}^{b-1}s_n(\varepsilon_n-\varepsilon_{n+1})+s_b\varepsilon_b\end{aligned}$$

$$\begin{aligned}\therefore\quad\left|\sum_{n=a}^{b}\gamma_n\varepsilon_n\right|&\leqslant\sum_{n=a}^{b-1}|s_n||\varepsilon_n-\varepsilon_{n-1}|+|s_b||\varepsilon_b|\\&\leqslant\max_{a\leqslant n\leqslant b}|s_n|\left(\sum_{a\leqslant n\leqslant b-1}|\varepsilon_n-\varepsilon_{n+1}|+|\varepsilon_b|\right)\end{aligned}$$

若此定理中 ε_n 是正的递减序列，则结论可改为

系 1 设 ε_n是正的递减序列，其他条件同定理 9·24，则

$$\left|\sum_{n=a}^{b}\gamma_n\varepsilon_n\right|\leqslant\max_{a\leqslant n\leqslant b}|s_n|\varepsilon_a \tag{40}$$

取 $\gamma_n=\chi(n)^*$，$\varepsilon_n=\frac{1}{n^s}(s>0)$有

系 2 若 $s>0$，则

$$\left|\sum_{n\geqslant a}\frac{\chi(n)}{n^s}\right|\leqslant\frac{1}{a^s} \tag{41}$$

故当 $s>0$ 时级数

$$\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s} \tag{42}$$

收敛。

证明 因为 $\chi(a)+\chi(a+1)+\chi(a+2)+\chi(a+3)=0$，所以

$$\left|\sum_{a\leqslant m\leqslant b}\chi(m)\right|\leqslant 1$$

由系 1 知道

$$\left|\sum_{n=a}^{b}\frac{\chi(n)}{n^s}\right|\leqslant\frac{1}{a^s}$$

因上式的结论与右边的 b 无关，故(41)成立，即(42)收敛。

定理9·25 设$r(k)$是 $x^2+y^2=k$ 的解数，π 是圆周率，

---

* 注意：这里的$\chi(n)$是如下的数论函数：

$$\chi(n)=\begin{cases}0, & \text{若}2\mid n\\ (-1)^{\frac{1}{2}(n-1)}, & \text{若}2\nmid n\end{cases}$$

并且，若 $n=\prod_{p\mid n}p^{\alpha}$为n的标准分解式，则$\delta(n)=\prod_{p\mid n}(1+\chi(p)+\chi(p^2)+\cdots+\chi(p^{\alpha}))$。

则

$$\sum_{1\leqslant k\leqslant x} r(k)=\pi x+O(\sqrt{x})$$

证明 由定理8·7及第八章等式(31)知道

$$\sum_{1\leqslant k\leqslant x} \gamma(k)=4\sum_{1\leqslant k\leqslant x}\delta(k)=4\sum_{1\leqslant k\leqslant x}\sum_{d\mid k}\chi(d)$$

$$=4\sum_{1\leqslant d\leqslant x}\chi(d)\sum_{\substack{1\leqslant k\leqslant x\\ d\mid k}}1$$

$$=4\sum_{1\leqslant k\leqslant x}\chi(d)\left[\frac{x}{d}\right]$$

其中$\left[\frac{x}{d}\right]$是不大于$\frac{x}{d}$的最大整数。将此和分成二部分，再应用定理9·24系 2，得

$$\sum\nolimits_1=4\sum_{1\leqslant n\leqslant\sqrt{x}}\chi(d)\left[\frac{x}{d}\right]$$

$$=4x\sum_{1\leqslant d\leqslant\sqrt{x}}\frac{\chi(d)}{d}+O(\sqrt{x})$$

$$=4x\sum_{d=1}^{\infty}\frac{\chi(d)}{d}+O(\sqrt{x})$$

$$=\pi x+O(\sqrt{x})$$

另一部分

$$\sum\nolimits_2=4\sum_{\sqrt{x}\leqslant d\leqslant x}\chi(d)\left[\frac{x}{d}\right]$$

由定理9·24系 1，得

$$\sum\nolimits_2=O(\sqrt{x})$$

$$\therefore \quad \sum_{1\leqslant k\leqslant x} r(k)=\pi x+O(\sqrt{x})$$

此定理可以简单地证明如下：显然 $\sum\limits_{1\leqslant k\leqslant x} r(k)$是适合

$$u^2+v^2\leqslant \chi$$

的整数对(u, v)的个数．即是中心在原点半径为$\sqrt{x}$的圆内（包括边界）整点的个数．该圆的面积等于 πx ．$\sqrt{x}$是一个正值函数，且$\left(\sum\limits_{1\leqslant k\leqslant x} r(k)-\pi\chi\right)/\sqrt{x}$是有界量，所以

$$\sum_{1\leqslant k\leqslant x} r(k)=\pi x+O(\sqrt{x})$$

事实上，在平面上过整点作 x 轴及 y 轴平行的直线，此诸直线将平面分成方格．圆内一个整点对应一个方格子，其四个顶点为(u, v)，$(u+1, v)$，$(u, v+1)$，$(u+1, v+1)$．如此所得的诸方格必在圆

$$u^2+v^2=(\sqrt{x}+\sqrt{2})^2 \qquad (\alpha)$$

之中，但一切半径为$\sqrt{x}$中心在原点的圆内全体整点包围了圆

$$u^2+v^2=(\sqrt{x}-\sqrt{2})^2 \qquad (\beta)$$

即这些格子的面积之和，必界于圆(α)与圆(β)的面积之间．

$$\therefore \quad \pi(\sqrt{x}-\sqrt{2})^2\leqslant \sum_{k\leqslant x} r(k)\leqslant \pi(\sqrt{x}+\sqrt{2})^2$$

即得定理．

由于 $h(-8)=1$，$h\left(\frac{-8}{4}\right)=h(-2)=0$，故 $d=-8$ 的型的类数为 1 ．故 $x^2+2y^2=k$ 的解数 $\psi(k)$，由定理 9·18 知$w=2$（对应于同一 1 的既约解的数目），又因克朗里克符号

$$\left(\frac{-8}{m}\right)=\left(\frac{-2}{m}\right)=\begin{cases}1, & 当\ m\equiv 1(\bmod 8)\\ 1, & 当\ m\equiv 3(\bmod 8)\\ -1, & 当\ m=5(\bmod 8)\\ -1, & 当\ m=7(\bmod 8)\end{cases}$$

与定理8·7的证法类似地可得$\psi(2^{\alpha}S)=\psi(S)$。故由定理9·22可得

定理9·26 S是奇数

$$x^2+2y^2=2^{\alpha}S \tag{43}$$

的解数是

$$2\sigma=2(\tau_1(k)+\tau_3(k)-\tau_5(k)-\tau_7(k)) \tag{44}$$

其中$\tau_i(k)$是s的正因数中同余于i的个数.

这个定理给出了椭圆(43)上的整点的个数。

同样地，应用定理9·18，9·22，9·26可以证明，双曲线上的整点数，

系1 $x^2+xy+y^2=k$ (45)

的解数为$6E(k)$，其中$E(k)$是k中形如$3h+1$的正因数的个数减去$3h+2$的正因数的个数。

系2 若m是奇数，则

$$x^2+3y^2=2^{\alpha}m \tag{46}$$

的解数

$$T=\begin{cases}0, & 若\alpha为正奇数\\ 6E(m), & 若\alpha为正偶数\\ 2E(m), & 若\alpha=0\end{cases}$$

$E(m)$的意义同系1。

证明 (i) 当α是正奇数时，若(46)有解，x，y必同为偶数，或同为奇数。若$x=2k+1$，$y=2h+1$，则

$x^2+3y^2=4(k^2+k+3h^2+3h+1) \Longrightarrow 2^\alpha m=2^\alpha m'$ (m'为奇数).故(46)无 x,y 同为奇数的解.若 $x=2k, y=2h$ 则 $x^2+3y^2=4(k^2+3h^2)$故右边是 2 的偶次方幂与奇数之积，故(46)亦无 x，y 同为偶数的解。即

$$T=0$$

(ii) 当 $\alpha=0$ 时，$k=2^0m=m$，$d=0^2-4\times1\times3=-12$由定理9·18知道(46)对应于某一 l 的解数$w=2$。

$$l\equiv-12(\bmod 4m),\ 0<l\leqslant 2m$$

的解数T'，由定理9·10的系知道

$$T'=\sum_{p\mid m}\left(\frac{d}{p}\right)=\sum_{p\mid m}\left(\frac{-12}{p}\right)=\sum_{p\mid m}\left(\frac{-3}{p}\right)$$

由第五章习题17知道，p 是$12k+1$或$12k+7$形的素数时，$\left(\frac{-3}{p}\right)=1$，p 是$12k+5$或$12k-1$形的素数时，$\left(\frac{-3}{p}\right)=-1$。而$p=3n+1$形的素数，当$n=4k+1$及$4k+3$时，$3n+1$是合数；当 $n=4k+2$ 或$4k$时，$p=12k+k$或$12k+1$可能是素数。同理 $p=3n+2$形的素数时，只可能是 $12k+5$ 或 $12k-1$形，所以

$$T=2T'=2\sum_{p\mid m}\left(\frac{-3}{p}\right)=2E(m)$$

(iii) 当$\alpha=2t(t>0)$时，若(46)有解，x，y 必同为偶数，或同为奇数。由于

$$\begin{aligned}(x_1^2+3y_1^2)(x_2^2+3y_2^2)&=(x_1x_2+3y_1y_2)^2\\&\quad+3(x_1y_2-x_2y_1)^2\\&=X^2+3Y^2\end{aligned}$$

所以(46)的解数是下列二方程解数 T_1，T_2 之积除以2：

$$x_1^2+3y_1^2=2^{2t},\quad x_2^2+3y_2^2=m$$

由(ii)知$T_2=2E(m)$，显然前一个方程有且只有 $x_1=\pm 2^t$，$y_1=0$及 $x_1=\pm 2^{t-1}$，$y_1=\pm 2^{t-1}$等六个解。所以

$$T=\frac{1}{2}T_1T_2=6E(m)$$

关于更一般的曲线，其内部整点的个数问题，捷克数学家M·V·Jarik 已给出了下面的定理：

定理9·27 命 l 表示一条有长的简单闭曲线的长度，A 表示该曲线所围区域的面积，N 为曲线内部所含整点的个数，则若 $l\geqslant 1$，必有

$$|A-N|<l.$$

要证明这个定理先证下面两个引理：

引理 1 在边长为 1 的正方形中，任作一两端点在正方形的周界上且与二对角线相交的连续曲线C，则C的长 $l\geqslant 1$。

证明 若C的两端点在正方形的一对对边上，则显然$l\geqslant 1$。

若C的端点在正方形的二相邻的边上（如图 1 ），易见

$$l\geqslant\overline{RP_1}+\overline{P_1Q_1}+\overline{Q_1T}$$

$$\geqslant\overline{AR}+\overline{RS}+\overline{SB}=\overline{AB}$$

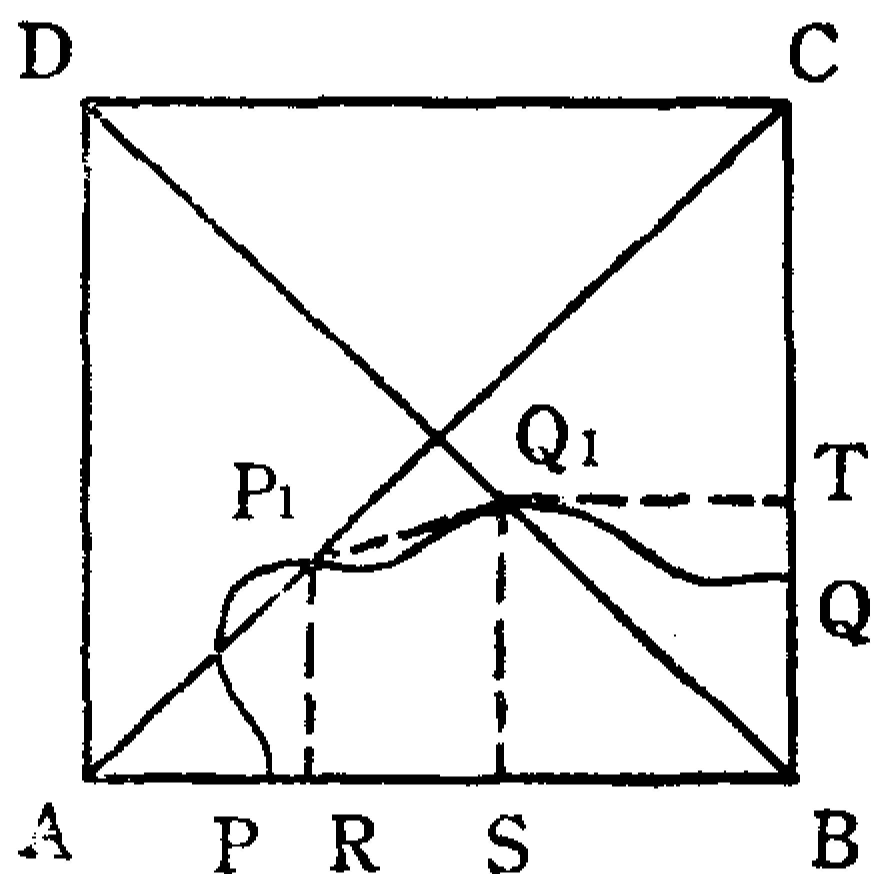


图 1

若C的两端点在正方形的同一边上，可同法证之。

引理 2 在边长为 1 的正方形中，作任一不通过正方形中心的连续曲线C，C的两端点在正方形的周界上。曲线C将正方形分为二部分，命Δ为其中不包含正方形中心O的一

部分，则Δ的面积必小于C的长度（数量关系）。

证明 分别考虑如图9·2的五种情形：

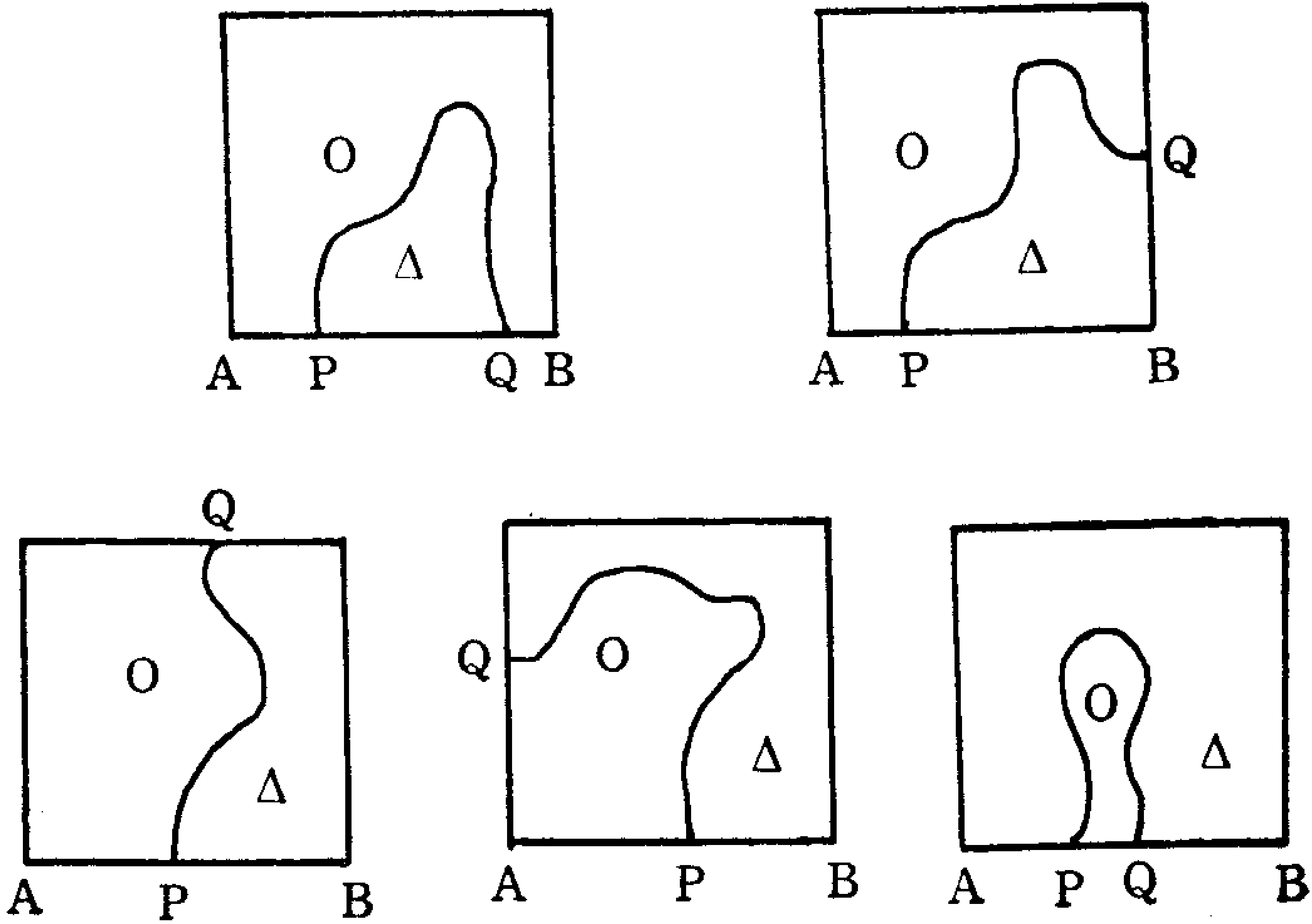


图 2

命O为正方形的中心，P，Q是曲线C的两个端点，S，l表示Δ的面积和C的长度，则在情形Ⅰ，Ⅱ中，易见从C上任一点到直线AB的距离必不能大于 l，故Δ全落在边长为1与 l 的矩形的内部，即 $S \leqslant 1 \cdot l = l$。在后三种情形中，由引理1知道 $l \geqslant 1$，所以有 $S \leqslant 1 \leqslant l$。

定理的证明：以 I 表示曲线所围成的区域，在平面上作网，以直线

$$x = m + \frac{1}{2},\quad y = n + \frac{1}{2}\ (m,\quad n = 0,\quad \pm 1,\quad \pm 2,\quad \cdots)$$

为经纬，网眼是边长为1的正方形，以Q_1，$Q_2 \cdots$，Q_k表示所有这些含有 I 的一部分的正方形的周界，而以C_i表示有长曲线在Q_i中的部分，以Ω_i表示Q_i与 I 的共通部分，而定义

$$N_i=\begin{cases}1, & \text{若 } \Omega_i \text{ 中有整点,}\\ 0, & \text{若 } \Omega_i \text{ 中无整点.}\end{cases}$$

又以A_i表示Ω_i的面积，l_i表示C_i的长度，于是若能证明

$$|A_i-N_i|<l_i$$

就可以了。

首先，我们考虑整个I都在Q中的情形，因为$I\geqslant 1$，故定理成立。因此，我们可以不失普遍性地假定I并不整个地处在一Q中，此时C_i为若干段曲线之和，而这些曲线段又将Q_i分为若干部分$D_i^{(s)}$。

若整点不在任何$D_i^{(s)}$中，以$A_i^{(s)}$表示$D_i^{(s)}$的面积，若$D_i^{(s)}$不在I中，则$N_i=1$，而$1-A_i\leqslant 1-A_i^{(s)}$，而由引理2，即得

$$1-A_i^{(s)}<l_i$$

于是得到定理的证明。

显然定理9·25可从定理9·27直接导出。

习　　题

1. 证明：$d=-36$时，有三个已化型：

$\{1, 0, 9\}$，$\{2, 2, 5\}$，$\{3, 0, 3\}$。

2 若x_0，y_0，z_0是不定方程

$$x^2+y^2+z^2=3xyz \tag{a}$$

的一个解(称为马可洛夫…Марков…数)，则

$$x_0,\ y_0,\ 3x_0y_0-z_0 \tag{b}$$

亦是(a)的一个解。

用这个方法写出$0<x\leqslant y\leqslant z<1000$的(a)的一切解。

3. 仿上题证明，若$(x_{1,0}, x_{2,0}, \cdots, x_{n,0})$是

$$x_1^2+x_2^2+\cdots+x_n^2=nx_1x_2\cdots x_n \tag{c}$$

的一个解，则

$$(x_{1,0},\ x_{2,0},\ \cdots,\ x_{n-1,0},\ (nx_{1,0}\cdots x_{n-1,0}-x_{n,0})) \tag{d}$$

亦是(c)的一解。

4 上题当 $n=4$时，求出 $0<x_1\leqslant x_2\leqslant x_3\leqslant x_4\leqslant 150$的一切解．

5 证明恒等式

$$y^{12}=(9x^4)^3+(3xy^3-9x^4)^3+(y^4-9x^3y)^3$$

从而得到：一数的12次幂可多种形式地表成三数的立方和．如，当 $y=5$，取 $x=1,\ 2,\ \cdots$有

$$5^{12}=9^3+366^3+580^3=144^3+606^3+265^3=\cdots.$$

6 证明：

$$w^3+3w(x^2+y^2+z^2)+6xyz=0 \tag{1}$$

的有理数解是

$$w=-6\rho abc,\ x=\rho a(a^2+3b^2+3c^2),$$
$$y=\rho b(a^2+3b^2+9c^2),\ z=3\rho c(a^2+b^2+3c^2). \tag{2}$$

其中$(a,\ b,\ c)=1$，ρ 是有理数。

7 应用上题，求

$$\alpha^3+\beta^3+\gamma^3+\delta^3=0 \tag{4}$$

的有理数解。

8 若 m 为奇数，则 $x^2+3y^2=4m$，有$E(m)$个正奇数解。其中$E(m)$如定理9·26系 2 中所定义的。

9 若把定义9·2推广为 mod q 相似：令$q>1$的素数，若有一整系数变换：

$$x=rX+sY,\ y=tX+uY\quad (ru-st,\ q)=1 \tag{1}$$

使

$$ax^2+bxy+cy^2\equiv a_1X^2+b_1XY+c_1Y^2\pmod q \tag{2}$$

则称二次型$\{a,\ b,\ c\}$与$\{a_1,\ b_1,\ c_1\}$mod q 相似.

(i) 若 d，d_1 分别是$\{a,\ b,\ c\}$与$\{a_1,\ b_1,\ c_1\}$ 的判别式，则

$$d_1\equiv(ru-st)^2d\pmod q \tag{3}$$

(ii) 若$\{a, b, c\}$与$\{a_1, b_1, c_1\}$ mod p (p是奇素数)，则

$$\left(\frac{d}{p}\right)=\left(\frac{d_1}{p}\right)$$

(iii) 若d是$\{a, b, c\}$的判别式，p是奇素数$p\nmid d$,则$\{a,b,c\}$必与一形如$\{a_1, o, c_1\}$的型 mod p 相似．下面诸小题当$p\nmid d$时都指$p\nmid ac$，$p|b$。

(iv) 若$p\nmid d$，则必有x，y使

$$ax^2+cy^2\equiv 1 \pmod p$$

(v) 若d是$\{a, b, c\}$的判别式，p是奇素数,$p\nmid d$，r是 mod p 的任一二次非剩余，则当$\left(\frac{d}{p}\right)=1$时，

$$\{a, b, c\}\sim\{1, 0, -1\}\sim\{0, 1, 0\} \pmod p$$

而当$\left(\frac{d}{p}\right)=-1$时，

$$\{a, b, c\}\sim\{1, 0, -r\} \pmod p$$

又$\{1, 0, -1\}$必不与$\{1, 0, -r\}$ mod p 相似。

(vi) 判别式相同的二次型必互相模p相似，其中p是不整除d的奇素数。

附　表

1. 4000以下的素数及其最小原根表

p	g	p	g	p	g	p	g	p	g	p	g	p	g
2	1	179	2	419	2	661	2	947	2	1229	2	1523	2
3	2	181	2	421	2	673	5	953	3	1231	3	1531	2
5	2	191	19	431	7	677	2	967	5	1237	2	1543	5
7	3	193	5	433	5	683	5	971	6	1249	7	1549	2
11	2	197	2	439	15	691	3	977	3	1259	2	1553	3
13	2	199	3	443	2	701	2	983	5	1277	2	1559	19
17	3	211	2	449	3	709	2	991	6	1279	3	1567	3
19	2	223	3	457	13	719	11	997	7	1283	2	1571	2
23	5	227	2	461	2	727	5	1009	11	1289	6	1579	3
29	2	229	6	463	3	733	6	1013	3	1291	2	1583	5
31	3	233	3	467	2	739	3	1019	2	1297	10	1597	11
37	2	239	7	479	13	743	5	1021	10	1301	2	1601	3
41	6	241	7	487	3	751	3	1031	14	1303	6	1607	5
43	3	251	6	491	2	757	2	1033	5	1307	2	1609	7
47	5	257	3	499	7	761	6	1039	3	1319	13	1613	3
53	2	263	5	503	5	769	11	1049	3	1321	13	1619	2
59	2	269	2	509	2	773	2	1051	7	1327	3	1621	2
61	2	271	6	521	3	787	2	1061	2	1361	3	1627	3
67	2	277	5	523	2	797	2	1063	3	1367	5	1637	2
71	7	281	3	541	2	809	3	1069	6	1373	2	1657	11
73	5	283	3	547	2	811	3	1087	3	1381	2	1663	3
79	3	293	2	557	2	821	2	1091	2	1399	13	1667	2
83	2	307	5	563	2	823	3	1093	5	1409	3	1669	2
89	3	311	17	569	3	827	2	1097	3	1423	3	1693	2
97	5	313	10	571	3	829	2	1103	5	1427	2	1697	3
101	2	317	2	577	5	839	11	1109	2	1429	6	1699	3
103	5	331	3	587	2	853	2	1117	2	1433	3	1709	3
107	2	337	10	593	3	857	3	1123	2	1439	7	1721	3
109	6	347	2	599	7	859	2	1129	11	1447	3	1723	3
113	3	349	2	601	7	863	5	1151	17	1451	2	1733	2
127	3	353	3	607	3	877	2	1153	5	1453	2	1741	2
131	2	359	7	613	2	881	3	1163	5	1459	5	1747	2
137	3	367	6	617	3	883	2	1171	2	1471	6	1753	7
139	2	373	2	619	2	887	5	1181	7	1481	3	1759	6
149	2	379	2	631	3	907	2	1187	2	1483	2	1777	5
151	6	383	5	641	3	911	17	1193	3	1487	5	1783	10
157	5	389	2	643	11	919	7	1201	11	1489	14	1787	2
163	2	397	5	647	5	929	3	1213	2	1493	2	1789	6
167	5	401	3	653	2	937	5	1217	3	1499	2	1801	11
173	2	409	21	659	2	941	2	1223	5	1511	11	1811	6

p	g	p	g	p	g	p	g	p	g	p	g	p	g
1823	5	2129	3	2417	3	2729	3	3049	11	3373	5	3691	2
1831	3	2131	2	2423	5	2731	3	3061	6	3389	3	3697	5
1847	5	2137	10	2437	2	2741	2	3067	2	3391	3	3701	2
1861	2	2141	2	2441	6	2749	6	3079	6	3407	5	3709	2
1867	2	2143	3	2447	5	2753	3	3083	2	3413	2	3719	7
1871	14	2153	3	2459	2	2767	3	3089	3	3433	5	3727	3
1873	10	2161	23	2467	2	2777	3	3109	6	3449	3	3733	2
1877	2	2179	7	2473	5	2789	2	3119	7	3457	7	3739	7
1879	6	2203	5	2477	2	2791	6	3121	7	3461	2	3761	3
1889	3	2207	5	2503	3	2797	2	3137	3	3463	3	3767	5
1901	2	2213	2	2521	17	2801	3	3163	3	3467	2	3769	7
1907	2	2221	2	2531	2	2803	2	3167	5	3469	2	3779	2
1913	3	2237	2	2539	2	2819	2	3169	7	3491	2	3793	5
1931	2	2239	3	2543	5	2833	5	3181	7	3499	2	3797	2
1933	5	2243	2	2549	2	2837	2	3187	2	3511	7	3803	2
1949	2	2251	7	2551	6	2843	2	3191	11	3517	2	3821	3
1951	3	2267	2	2557	2	2851	2	3203	2	3527	5	3823	3
1973	2	2269	2	2579	2	2857	11	3209	3	3529	17	3833	3
1979	2	2273	3	2591	7	2861	2	3217	5	3533	2	3847	5
1987	2	2281	7	2593	7	2879	7	3221	10	3539	2	3851	2
1993	5	2287	19	2609	3	2887	5	3229	6	3541	7	3853	2
1997	2	2293	2	2617	5	2897	3	3251	6	3547	2	3863	5
1999	3	2297	5	2621	2	2903	5	3253	2	3557	2	3877	2
2003	5	2309	2	2633	3	2909	2	3257	3	3559	3	3881	13
2011	3	2311	3	2647	3	2917	5	3259	3	3571	2	3889	11
2017	5	2333	2	2657	3	2927	5	3271	3	3581	2	3907	2
2027	2	2339	2	2659	2	2939	2	3299	2	3583	3	3911	13
2029	2	2341	7	2663	5	2953	13	3301	6	3593	3	3917	2
2039	7	2347	3	2671	7	2957	2	3307	2	3607	5	3919	3
2053	2	2351	13	2677	2	2963	2	3313	10	3613	2	3923	2
2063	5	2357	2	2683	2	2969	3	3319	6	3617	3	3929	3
2069	2	2371	2	2687	5	3971	10	3323	2	3623	5	3931	2
2081	3	2377	5	2689	19	2999	17	3329	3	3631	21	3943	3
2083	2	2381	3	2693	2	3001	14	3331	3	3637	2	3947	2
2087	5	2383	5	2699	2	3011	2	3343	5	3643	2	3967	6
2889	7	2389	2	2707	2	3019	2	3347	2	3659	2	3989	2
2099	2	2393	3	2711	7	3023	5	3359	11	3671	13		
2111	7	2399	11	2713	5	3037	2	3361	22	3673	5		
2113	5	2411	6	2719	3	3041	3	3371	2	3677	2		

2. 100以内素数的元根及指数表

素数 5

元根：2，3。

底数： 2

I

N.	1	2	3	4
I.	4	1	3	2

N

I.	1	2	3	4
N.	2	4	3	1

素数 7

元根：3，5。

底数： 3

I

N.	1	2	3	4	5	6
I.	6	2	1	4	5	3

N

I.	1	2	3	4	5	6
N.	3	2	6	4	5	1

素数11

元根：2，6，7，8。

底数： 2

I

N.	1	2	3	4	5	6	7	8	9	10
I.	10	1	8	2	4	9	7	3	6	5

N

I.	1	2	3	4	5	6	7	8	9	10
N.	2	4	8	5	10	9	7	3	6	1

素数13

元根：2，6，7，11

底数：6

I

N	0	1	2	3	4	5	6	7	8	9
0		12	5	8	10	9	1	7	3	4
1	2	11	6							

N

I	0	1	2	3	4	5	6	7	8	9
0		6	10	8	9	2	12	7	3	5
1	4	11	1							

素数17

元根：3，5，6，7，10，11，12，14

底数：10

I

N	0	1	2	3	4	5	6	7	8	9
0		16	10	11	4	7	5	9	14	6
1	1	13	15	12	3	2	8			

N

I	0	1	2	3	4	5	6	7	8	9
0		10	15	14	4	6	9	5	16	7
1	2	3	13	11	8	12	1			

素数19

元根：2，3，10，13，14，15.

底数：10

I

N	0	1	2	3	4	5	6	7	8	9
0		18	17	5	16	2	4	12	15	10
1	1	6	3	13	11	7	14	8	9	

N

I	0	1	2	3	4	5	6	7	8	9
0		10	5	12	6	3	11	15	17	18
1	9	14	7	13	16	8	4	2	1	

素数23

元根：5，7，10，11，14，15，17，19，20，21.

底数：10

I

N	0	1	2	3	4	5	6	7	8	9
0		22	8	20	16	15	6	21	2	18
1	1	3	14	12	7	13	10	17	4	5
2	9	19	11							

N

I	0	1	2	3	4	5	6	7	8	9
0		10	8	11	18	19	6	14	2	20
1	16	22	13	15	12	5	4	17	9	21
2	3	7	1							

素数29

元根：2，3，8，10，11，14，15，18，19，21，26，27.

底数：10

I

N	0	1	2	3	4	5	6	7	8	9
0		28	11	27	22	18	10	20	5	26
1	1	23	21	2	3	17	16	7	9	15
2	12	19	6	24	4	8	13	25	14	

N

I	0	1	2	3	4	5	6	7	8	9
0		10	13	14	24	8	22	17	25	18
1	6	2	20	26	28	19	16	15	5	21
2	7	12	4	11	23	27	9	3	1	

素数31

元根：3，11，12，13，17，21，22，24.

底数：17

I

N	0	1	2	3	4	5	6	7	8	9
0		30	12	13	24	20	25	4	6	26
1	2	29	7	23	16	3	18	1	8	22
2	14	17	11	21	19	10	5	9	28	27
3	15									

N

I	0	1	2	3	4	5	6	7	8	9
0		17	10	15	7	26	8	12	18	27
1	25	22	2	3	20	30	14	21	16	24
2	5	23	19	13	4	6	9	29	28	11
3	1									

素数37

元根：2，5，13，15，17，18，19，20，22，24，32，35。

底数：5

I

N	0	1	2	3	4	5	6	7	8	9
0		36	11	34	22	1	9	28	33	32
1	12	6	20	13	3	35	8	5	7	25
2	23	26	17	21	31	2	24	30	14	15
3	10	27	19	4	16	29	18			

N

I	0	1	2	3	4	5	6	7	8	9
0		5	25	14	33	17	11	18	16	6
1	30	2	10	13	28	29	34	22	36	32
2	12	23	4	20	26	19	21	31	7	35
3	27	24	9	8	3	15	1			

素数41

元根：6，7，11，12，13，15，17，19，22，24，26，28，29，30，34，35。

底数：6

I

N	0	1	2	3	4	5	6	7	8	9
0		40	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9
2	34	14	29	36	13	4	17	5	11	7
3	23	28	10	18	19	21	2	32	35	6
4	20									

N

I	0	1	2	3	4	5	6	7	8	9
0		6	36	11	25	27	39	29	10	19
1	32	28	4	24	21	3	18	26	33	34
2	40	35	5	30	16	14	2	12	31	22
3	9	13	37	17	20	38	23	15	8	7
4	1									

素数43

元根：3，5，12，18，19，20，26，28，29，30，33，34。

底数：28

I

N	0	1	2	3	4	5	6	7	8	9
0		42	39	17	36	5	14	7	33	34
1	2	6	11	40	4	22	30	16	31	29
2	41	24	3	20	8	10	37	9	1	25
3	19	32	27	23	13	12	28	35	26	15
4	38	18	21							

I	0	1	2	3	4	5	6	7	8	9
0		28	10	22	14	5	11	7	24	27
1	25	12	35	34	6	39	17	3	41	30
2	23	42	15	33	21	29	38	32	36	19
3	16	18	31	8	9	37	4	26	40	2
4	13	20	1							

素数47

元根：5，10，11，13，15，19，20，22，23，26，29，30，31，33，35，38，39，40，41，43，44，45。

底数：10

I

N	0	1	2	3	4	5	6	7	8	9
0		46	30	18	14	17	2	38	44	36
1	1	27	32	3	22	35	28	42	20	29
2	31	10	11	39	16	34	33	8	6	43
3	19	5	12	45	26	9	4	24	13	21
4	15	25	40	37	41	7	23			

N

I	0	1	2	3	4	5	6	7	8	9
0		10	6	13	36	31	28	45	27	35
1	21	22	32	38	4	40	24	5	3	30
2	18	39	14	46	37	41	34	11	16	19
3	2	20	12	26	25	15	9	43	7	23
4	42	44	17	29	8	33	1			

素数53

元根：2，3，5，8，12，14，18，19，20，21，22，26，27，31，32，33，34，35，39，41，45，48，50，51。

底数：26

I

N	0	1	2	3	4	5	6	7	8	9
0		52	25	9	50	31	34	38	23	18
1	4	46	7	28	11	40	48	42	43	41
2	29	47	19	39	32	10	1	27	36	6
3	13	45	21	3	15	17	16	22	14	37
4	2	33	20	30	44	49	12	8	5	24
5	35	51	26							

N

I	0	1	2	3	4	5	6	7	8	9
0		26	40	33	10	48	29	12	47	3
1	25	14	46	30	38	34	36	35	9	22
2	42	32	37	8	49	2	52	27	13	20
3	43	5	24	41	6	50	28	39	7	23
4	15	19	17	18	44	31	11	21	16	45
5	4	51	1							

素数59

元根：2，6，8，10，11，13，14，18，23，24，30，31，32，33，34，37，38，39，40，42，43，44，47，50，52，54，55，56。

底数：10

I

N	0	1	2	3	4	5	6	7	8	9
0		58	25	32	50	34	57	44	17	6
1	1	45	24	23	11	8	42	14	31	22
2	26	18	12	27	49	10	48	38	36	4
3	33	7	9	19	39	20	56	41	47	55
4	51	2	43	13	37	40	52	53	16	30
5	35	46	15	28	5	21	3	54	29	

N

I	0	1	2	3	4	5	6	7	8	9
0		10	41	56	29	54	9	21	15	32
1	25	14	22	43	17	52	48	8	21	33
2	35	55	19	13	12	2	20	23	53	58
3	49	18	3	30	5	50	28	44	27	34
4	45	37	16	42	7	11	51	38	26	24
5	4	40	46	47	57	39	36	6	1	

素数61

元根：2，6，7，10，17，18，26，30，31，35，43，44，51，54，55，59.

底数：10

I

N	0	1	2	3	4	5	6	7	8	9
0		60	47	42	34	14	29	23	21	24
1	1	45	16	20	10	56	8	49	11	22
2	48	5	32	39	3	28	7	6	57	25
3	43	13	55	27	36	37	58	33	9	2
4	35	18	52	41	19	38	26	40	50	46
5	15	31	54	51	53	59	44	4	12	17
6	30									

N

I	0	1	2	3	4	5	6	7	8	9
0		10	39	24	57	21	27	26	16	38
1	14	18	58	31	5	50	12	59	41	44
2	13	8	19	7	9	29	46	33	25	6
3	60	51	22	37	4	40	34	35	45	23
4	47	43	3	30	56	11	49	2	20	17
5	48	53	42	54	52	32	15	28	36	55
6	1									

素数67

元根：2，7，11，12，13，18，20，28，31，32，34，41，44，46，48，50，51，57，61，63.

底数：12

I

N	0	1	2	3	4	5	6	7	8	9
0		66	29	9	59	39	38	7	21	18
1	2	61	1	23	36	48	50	8	47	26
2	31	16	24	20	30	12	52	27	65	22
3	11	43	13	4	37	46	10	44	55	32
4	60	19	45	63	53	57	49	64	59	14
5	41	17	15	3	56	34	28	35	51	54
6	40	5	6	25	42	62	33			

N

I	0	1	2	3	4	5	6	7	8	9
0		12	10	53	33	61	62	7	17	3
1	36	30	25	32	49	52	21	51	9	41
2	23	8	29	13	22	63	19	27	56	2
3	24	20	39	66	55	57	14	34	6	5
4	60	50	64	31	37	42	35	18	15	46
5	16	58	26	44	59	38	54	45	4	48
6	40	11	65	43	47	28	1			

素数71

元根：7，11，13，21，22，28，31，33，35，42，44，47，52，53，55，56，59，61，62，63，65，67，68，69.

底数：62

I

N	0	1	2	3	4	5	6	7	8	9
0		70	58	18	46	14	6	33	34	36
1	2	43	64	27	21	32	22	7	24	38
2	60	51	31	5	52	28	15	54	9	4
3	20	13	10	61	65	47	12	30	26	45
4	48	55	39	44	19	50	63	17	40	66
5	16	25	3	59	42	57	67	56	62	29
6	8	37	1	69	68	41	49	11	53	23
7	35									

N

I	0	1	2	3	4	5	6	7	8	9
0		62	10	52	29	23	6	17	60	28
1	32	67	36	31	5	26	50	47	3	44
2	30	14	16	69	18	51	38	13	25	59
3	37	22	15	7	8	70	9	61	19	42
4	48	65	54	11	43	39	4	35	40	66
5	45	21	24	68	27	41	57	55	2	53
6	20	33	58	46	12	34	49	56	64	63
7	1									

素数73

元根：5，11，13，14，15，20，26，28，29，31，33，34，39，40，42，44，45，47，53，58，59，60，62，68.

底数：5

I

N	0	1	2	3	4	5	6	7	8	9
0		72	8	6	16	1	14	33	24	12
1	9	55	22	59	41	7	32	21	20	62
2	17	39	63	46	30	2	67	18	49	35
3	15	11	40	61	29	34	28	64	70	65
4	25	4	47	51	71	13	54	31	38	66
5	10	27	3	53	26	56	57	68	43	5
6	23	58	19	45	48	60	69	50	37	52
7	42	44	36							

N

I	0	1	2	3	4	5	6	7	8	9
0		5	25	52	41	59	3	15	2	10
1	50	31	9	45	6	30	4	20	27	62
2	18	17	12	60	8	40	54	51	36	34
3	24	47	16	7	35	29	72	68	48	21
4	32	14	70	58	71	63	23	42	64	28
5	67	43	69	53	46	11	55	56	61	13
6	65	33	19	22	37	39	49	26	57	66
7	38	44	1							

素数79

元根：3，6，7，28，29，30，34，35，37，39,43,47，48，53，54，59，60，63，66,68,70,74,75,77。

底数：29

I

N	0	1	2	3	4	5	6	7	8	9
0		78	50	71	22	34	43	19	72	64
1	6	70	15	74	69	27	44	9	36	10
2	56	12	42	52	65	68	46	57	41	1
3	77	76	16	63	59	53	8	23	60	67
4	28	21	62	47	14	20	24	55	37	38
5	40	2	18	7	29	26	13	3	51	17
6	49	75	48	5	66	30	35	54	31	45
7	25	33	58	4	73	61	32	11	39	

N

I	0	1	2	3	4	5	6	7	8	9
0		29	51	57	73	63	10	53	36	17
1	19	77	21	56	44	12	32	59	52	7
2	45	41	4	37	46	70	55	15	40	54
3	65	68	76	71	5	66	18	48	49	78
4	50	28	22	6	16	69	26	43	62	60
5	2	58	23	35	67	47	20	27	72	34
6	38	75	42	33	9	24	64	39	25	14
7	11	3	8	74	13	61	31	30	1	

素数83

元根：2，5，6，8，13，14，15，18，19，20，22，24 32，34，35，39，42，43，45，46，47，50,52，53，54，55，56，57，58，60，62，66，67,71，72，73，74，76，79，80。

底数：50

I

N	0	1	2	3	4	5	6	7	8	9
0		82	3	52	6	81	55	24	9	22
1	2	72	58	67	27	51	12	4	25	59
2	5	76	75	16	61	80	70	74	30	36
3	54	32	15	42	7	23	28	60	62	37
4	8	38	79	49	78	21	19	69	64	48
5	1	56	73	13	77	71	33	29	39	20
6	57	34	35	46	18	66	45	53	10	68
7	26	17	31	43	63	50	65	14	40	47
8	11	44	41							

N

I	0	1	2	3	4	5	6	7	8	9
0		50	10	2	17	20	4	34	40	8
1	68	80	16	53	77	32	23	71	64	46
2	59	45	9	35	7	18	70	14	6	57
3	28	72	31	56	61	62	29	39	41	58
4	78	82	33	73	81	66	63	79	49	43
5	75	15	3	67	30	6	51	60	12	19
6	37	24	38	74	48	76	65	13	69	47
7	26	55	11	52	27	22	21	54	44	42
8	25	5	1							

素数89

元根：3,6,7,13,14,15,19,23,24,26,27,28,29,30,31,33,35,38,41,43,46,48,51,54,56,58,59,60,61,62, 63, 65, 66,70,74, 75, 76, 82, 83, 86.

底数：30

I

N	0	1	2	3	4	5	6	7	8	9
0		88	72	87	56	18	71	7	40	86
1	2	4	55	65	79	17	24	82	70	53
2	74	6	76	31	39	36	49	85	63	29
3	1	57	8	3	66	25	54	77	37	64
4	58	67	78	59	60	16	15	34	23	14
5	20	81	33	10	69	22	47	52	13	45
6	73	19	41	5	80	83	75	32	50	30
7	9	26	38	68	61	35	21	11	48	46
8	42	84	51	27	62	12	43	28	44	

N

I	0	1	2	3	4	5	6	7	8	9
0		30	10	33	11	63	21	7	32	70
1	53	77	85	58	49	46	45	15	5	61
2	50	76	55	48	16	35	71	83	87	29
3	69	23	67	52	47	75	25	38	72	24
4	8	62	80	86	88	59	79	56	78	26
5	68	82	57	19	36	12	4	31	40	43
6	44	74	84	28	39	13	34	41	73	54
7	18	6	2	60	20	66	22	37	42	14
8	64	51	17	65	81	27	9	3	1	

素数97

元根：5, 7, 10, 13, 14, 15, 17, 21, 23, 26, 29, 37, 38, 39, 40, 41, 56, 57, 58, 59, 60,68, 71, 74, 76, 80, 82, 83, 84, 87, 90, 92.

底数：10

I

N	0	1	2	3	4	5	6	7	8	9
0		96	86	2	76	11	88	53	66	4
1	1	82	78	83	43	13	56	19	90	27
2	87	55	72	79	68	22	73	6	33	47
3	3	26	46	84	9	64	80	41	17	85
4	77	71	45	44	62	15	69	60	58	10
5	12	21	63	14	92	93	23	29	37	65
6	89	32	16	57	36	94	74	51	95	81
7	54	25	70	20	31	24	7	39	75	42
8	67	8	61	91	35	30	34	49	52	18
9	5	40	59	28	50	38	48			

N

I	0	1	2	3	4	5	6	7	8	9
0		10	3	30	9	90	27	76	81	34
1	49	5	50	15	53	45	62	38	89	17
2	73	51	25	56	75	71	31	19	93	57
3	85	74	61	28	86	84	64	58	95	77
4	91	37	79	14	43	42	32	29	96	87
5	94	67	88	7	70	21	16	63	48	92
6	47	82	44	52	35	59	8	80	24	46
7	72	41	22	26	66	78	4	40	12	23
8	36	69	11	13	33	39	2	20	6	60
9	18	83	54	55	65	68	1			

习 题 解 答

第 一 章

1.（i） 当 n 为任一整数时，n 和 $n+1$ 必一奇一偶，故 $2|n(n+1)$。若 $3|n(n+1)$，则命题正确；否则 $n=3m+1$，m 为整数，则 $2n+1=2(3m+1)+1=6m+3\Longrightarrow 3|2n+1$。

$\therefore\quad 6|n(n+1)(2n+1)$。

（ii） 与前题同样地讨论知道，$2|n(n-1)$；若 $3|n(n-1)$，则命题正确。否则 $n=3m+2$，m 为整数，则 $2n-1=2(3m+2)-1=6m+3$

$\therefore\quad 6|n(n-1)(2n-1)$。

（iii） $\because\quad (2m+1)^2-1=4m(m+1)$，

而 $2|m(m+1)$，故 $8|[(2m+1)^2-1]$。

（iv） 与（i）、（ii）同样地，$2|n(n+1)$，若 $3|n(n+1)$，则命题正确，否则 $n=3m+1$（m 是整数）$\Longrightarrow 3|n+2$。

$\therefore\quad 6|n(n+1)(n+2)$。

或者说，三个连续整数必被 3 整除，两个连续整数必被 2 整除，又 2 与 3 互素，故 6 整除 $n(n+1)(n+2)$。

2 设 $a=a_n\cdot 10^n+a_{n-1}\cdot 10^{n-1}+\cdots+a_1\cdot 10+a_0$，其中 a_0，a_1，…，$a_n\neq 0$ 是 0 到 9 中一个数字。

（i） 因为 $2|10^i(i=1,\cdots,n)$，所以 $2|a\Longleftrightarrow 2|a_0$。

（ii） 因为 $5|10^i(i=1,\cdots,n)$，所以 $5|a\Longleftrightarrow 5|a_0$，即 $a_0=5$ 或 $a_0=0$。

（iii） 因为 $10^i=3q_i+1$，$10^i=9q_i'+1$（q_i，q_i' 是整数，$i=1,\cdots,n$） 所以

$$a=(a_nq_n+\cdots+a_1q_1)\times 3+(a_n+\cdots+a_1+a_0),$$

或

$$a=a_nq_n'+\cdots+a_1q_1')\times 9+(a_n+\cdots+a_1+a_0).$$

$\therefore\quad 3|a$（或 $9|a$）$\Longleftrightarrow 3|a_n+\cdots+a_1+a_0$（或 $9|a_n+\cdots+a_0$

3　$n(n+1)(n+2)(n+3)+1=(n^2+3n)(n^2+3n+2)+1$

$=(n^2+3n)^2+2(n^2+3n)+1=(n^2+3n+1)^2$。

其中n为任意正整数。

事实上，本题n可推广为任意整数。

4　设$a=2m+1$，由第一题（iii）知道$8|a^2-1$；又$a(a^2-1)=(a-1)a(a+1)$，由第一题(iv)知道，$6|a(a^2-1)$，所以$[6,8]|(a^2-1)$，即$24|a(a^2-1)$。

5　因为$2\nmid a$且$3\nmid a$，所以$a=6k\pm1$，

$\therefore$　$a^2+23=(6k\pm1)^2+23=12k(3k\pm1)+24$

若$k=2m$为偶数时，则$24|a^2+23$；

若$k=2m+1$为奇数时，则$(3k\pm1)=6m+3\pm1$是偶数，故

$24|a^2-23$。

6　今用数学归纳法证明之

A）　当$n=1$时，$s_1=3+\sqrt{5}+3-\sqrt{5}=6$，$2|6$；当$n=2$时，$s_2-(3+\sqrt{5})^2+(3-\sqrt{5})^2=28$，$2^2|28$。所以$n=1$，2时，命题正确。

B）　设$n\leqslant k$时命题正确，当$n=k+1$时，令$3+\sqrt{5}=a$，$3-\sqrt{5}=b$，则

$s_{k+1}=a^{k+1}+b^{k+1}=a^{k+1}+ba^k+b^{k+1}+ab^k-ab^k-ba^k$

$=(a+b)(a^k+b^k)-ab(a^{k-1}+b^{k-1})$，

由归纳法假设知，$2^{k+1}|(a+b)(a^k+b^k)$，$2^{k-1}|a^{k-1}+b^{k-1}$，而$ab=(3+\sqrt{5})(3-\sqrt{5})=4\Longrightarrow 2^{k+1}|abs_{k-1}$

$\therefore$　$2^{k+1}|s_{k+1}$

所以n为任意正整数时，都有$2^n|s_n$。

7　$5^n+2\times3^{n-1}+1=5^n+3^n-(3^{n-1}-1)=(5+3)(5^{n-1}-5^{n-2}\times3+\cdots+3^{n-1})-(3^2-1)(9^{\frac{n-1}{2}-1}+9^{\frac{n-1}{2}-2}+\cdots+1)=8k$（k为整数）。

8　(i)　$5^{2n+1}\cdot2^{n+2}+3^{n+2}\cdot2^{2n+1}=20\cdot50^n+18\cdot12^n=$

$= 38 \cdot 50^n - 18(50^n - 12^n) = 38k$（k是整数）

(ii) $2^{6n+9} - 5^{2n+1} = 512 \times 64^n - 5 \times 25^n = 507 \times 64^n + 5(64^n - 25^n) = 39 \times 13 \times 64^n + 5 \times 39(64^{n-1} + \cdots + 25^{n-1}) = 39k$

（k是整数）。

(iii) 用数学归纳法证明之，

A) 当$n=1$时，结论正确，因为$2^6 - 7 + 41 = 98 = 2 \times 49$。

B) 设为$n-1$时，结论正确，则

$2^{3n+3} - 7n + 41 = 2^{3(n-1)+3} \cdot 2^3 - 7(n-1) + 41 - 7$

$= 49t + 7(2^{3n} - 1) = 49k$（k是整数）。

9 (i) $n^5 - n = (n-1)n(n+1)(n^2+1)$

由第一题（iv）知道$6|n^5-n$，若$5|(n-1)n(n+1)$，则已证明；否则$n = 5m \pm 2 \Longrightarrow n^2 + 1 = 5m(5m \pm 4) + 5 = 5k$（k是整数）。

$\therefore$ $30|n^5 - n$。

(ii) $T = n^2(n^2-1)(n^2-4) = (n-2)(n-1)n^2(n+1)(n+2)$，五个连续整数必有一个是5的倍数，故$5|T$，又由第一题（iv）知道$6|(n-2)(n-1)n$，$6|n(n+1)(n+2) \Longrightarrow 9|T$，$4|T$。当n为偶数时，显然$8|T$；当$n = 2m+1$为奇数时，$8|n^2-1$（$\because n^2 - 1 = 4m(m+1)$），即$8|T$。由于8，9，5两两互素

$\therefore$ $360|n^5 - n$。

(iii)$n^3 + 1|n = n^3 - n + 12n = (n-1)n(n+1) + 12n = 6k$（k是整数）。

10 (i) $n^{n-1} - 1 = [(n-1)+1]^{n-1} - 1 = \{(n-1)^{n-1} + C_{n-1}^1 (n-1)^{n-2} + \cdots + C_{n-1}^{n-2}(n-1) + 1\} - 1$

$$= (n-1)^{n-1} + (n-1)^{n-1} + \cdots + (n-1)^2. \qquad (\alpha)$$

当$n=1$，2时，$0|0$，$1|1$，故结论正确。当$n>2$时，(α)右边每一项都被$(n-1)^2$所整除。故结论正确。

(ii) A) 当$n=1$时，$n^3 + (n+1)^3 + (n-1)^3 = 9$。

B) 设$n=k$时，$9|k^3 + (k+1)^3 + (k-1)^3$。当$n=k+1$时，

$(k+1)^3 + (k+2)^3 + k^3 = k^3 + (k+1)^3 + [(k-1)+3]^3 =$

$$=[k^3+(k+1)^3+(k-1)^3]+9(k-1)^2+27(k-1)+3^3$$

$=9k$（k是整数）.

11　(i)

4	48	84	120
3	12	21	30
2	4	7	10
	2	7	5

注意：上面“除法”中用“实线”时，表示除数是各被除数的公因数；用“虚线”时，表示除数是被除数中至少二数的公因数，但不是一切被除数的公因数。这样求诸数的最大公因数，就是“实线”部分诸除数之积；最小公倍数就是诸除数及最后一列诸“商”之积。

$\therefore$ $(48,\ 84,\ 120)=4\times3=12$；

$[48,\ 84,\ 120]=4\times3\times2\times2\times7\times5=1680$

(ii)

2	360	810	1260	3150
45	180	405	630	1575
2	4	9	14	35
7	2	9	7	35
	2	9	1	5

$\therefore$ $(360,\ 810,\ 1260,\ 3150)=2\times45=90$；

$[360,\ 810,\ 1260,\ 3150]=2\times45\times2\times7\times2\times9\times1\times5=11340$.

12

3	51425	13310	1
	39930	11495	
6	11495	1815	3
	10890	1815	
	605	0	

$\therefore$ $(51425, 13310)=605$；$[51425, 13310]=\dfrac{51425\times13310}{605}=$

$=1131350$。

13　因为$(54, 48, 72)=6$，所以每组6人，甲班共$54\div6$ 9（组），乙班共$48\div6=8$（组），两班共$72\div6=12$（组）。

14　先求$[84, 36, 60, 48]=5040$，

甲转$\dfrac{5040}{84}=60$（圈）；

乙转　$5040\div36=140$（圈）；

丙转　$5040\div60=84$（圈）；

丁转　$5040\div48=105$（圈）。

15　若$\left(\dfrac{m}{a_1}, \dfrac{m}{a_2}, \cdots, \dfrac{m}{a_n}\right)=1$，而$[a_1, a_2, \cdots, a_n]=m'$，因为m是$a_1, a_2, \cdots\cdots, a_n$的一个公倍数，所以$m'|m$，即$m=m'k$ $(k\geqslant1)$，

$$\therefore\quad 1=\left(\frac{m}{a_1}, \frac{m}{a_2}, \cdots, \frac{m}{a_n}\right)=\left(\frac{m'k}{a_1}, \frac{m'k}{a_2}, \cdots, \frac{m'k}{a_n}\right)$$

$$=\left(\frac{m'}{a_1}, \frac{m'}{a_2}, \cdots, \frac{m'}{a_n}\right)k$$

$$=kd\Longrightarrow k=1,\ d=1\Longrightarrow m=m'=[a_1, a_2, \cdots, a_n].$$

反之，若$[a_1, a_2, \cdots, a_n]=m$，则$\dfrac{m}{a_1}, \dfrac{m}{a_2}, \cdots, \dfrac{m}{a_n}$都是正整数。如果$\left(\dfrac{m}{a_1}, \dfrac{m}{a_2}, \cdots, \dfrac{m}{a_n}\right)=d$，那末$m=a_1k_1d=a_2k_2d=\cdots=a_nk_nd$，$d|m\Longrightarrow m=m_1d\Longrightarrow m_1|m$，又因$m_1$是$a_1, a_2, \cdots, a_n$的公倍数$\Longrightarrow m|m_1$

$\therefore$　$m=m_1$，$d=1$。

16　因为m的任一正因数，必是形如

$$p_1^{\beta_1}p_2^{\beta_2}\cdots p_n^{\beta_n}(0\leqslant\beta_i\leqslant\alpha_i;\ i=1, 2, \cdots, n)$$

的数，而β_i的取值共有α_i+1种方法$(i=1, 2, \cdots, n)$，所以m的正因数共有

$$\tau(m)=(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_n+1)$$

个。

$96=2^5\times 3 \Longrightarrow \tau(96)=(5+1)(1+1)=12$;

$168=2^3\times 3\times 7 \Longrightarrow \tau(168)=(3+1)(1+1)(1+1)=16$;

$255=5\times 3\times 7 \Longrightarrow \tau(255)=(1+1)(1+1)(1+1)=8$

因为12! 中出现2，3，5，7，11的方次数，分别是：

$$\alpha_1=\left[\frac{12}{2}\right]+\left[\frac{12}{4}\right]+\left[\frac{12}{8}\right]=10;$$

$$\alpha_2=\left[\frac{12}{3}\right]+\left[\frac{12}{9}\right]=5;$$

$$\alpha_3=\left[\frac{12}{5}\right]=2;\quad \alpha_4=\left[\frac{12}{7}\right]=1;\quad \alpha_5=\left[\frac{12}{11}\right]=1.$$

$\therefore\ \tau(12!)=(10+1)(5+1)(2+1)(1+1)(1+1)=792$。

17　因为m的任一正因数，都是形如 $p_1^{\beta_1}\cdots p_n^{\beta_n}$ 的数，其中 $\beta_i=0,\ 1,\ \cdots,\ \alpha_i(i=1,\ \cdots,\ n)$

$$\therefore\ s(m)=(1+p_1+\cdots+p_1^{\alpha_1})\cdots(1+p_n+\cdots+p_n^{\alpha_n})$$

$$=\frac{p_1^{\alpha_1-1}-1}{p_1-1}\cdots\frac{p_n^{\alpha_n-1}-1}{p_n-1}.$$

18　形如$4n-1$的整数中，必有形如 $4m-1$ 的素因子，事实上，如果$4n-1$的一切因子都是 $4m+1$ 形时，那末 $4n-1=(4m_1+1)(4m_2+1)\cdots(4m_s+1)=4k+1$，其中k是$m_1$，$m_2$，…，$m_s$的整系数多项式，所以是一个整数，这是不可能的。

设形如$4n-1$的素数只有有限个 p_1，p_2，…，p_s。令

$$a=4p_1\cdots p_s-1,$$

则p_i（$i=1$，…，s）不整除a，所以 a 有异于p_1，…，p_s的形如$4n-1$的素因子。

19　除 2 和 3 外的任一素数都是$6n+1$或$6n+5$形，令

$$q=2\cdot 3\cdot 5\cdot\cdots p-1$$

小于或等于p的素数都不整除q，因此存在大于p并且整除q的素数，并

且有6n + 5形的素数整除q。事实上，若全是6n + 1形的素数，则它们之积仍是6n + 1形，这是不可能的。

20　设F_n和F_{n+k}（$k>0$）是两个费马数，并且$m\mid F_n$，$m\mid F_{n+k}$

若$x=2^{2^n}$，我们有

$$\frac{F_{n+k}-2}{F_n}=\frac{2^{2^{n+k}}-1}{2^{2^n}+1}=\frac{x^{2^k}-1}{x+1}=x^{2^k-1}-x^{2^k-2}+\cdots-1,$$

因而$F_n\mid F_{n+k}-2$。所以

$m\mid F_{n+k}$，$m\mid F_{n+k}-2\Longrightarrow m\mid 2$

由于F_n是奇数，故$m=1$。所以$(F_n,\ F_{n+k})=1$

21　$a_1=[e]=2$，$\{e\}=0.71828182845904\cdots$；

$a_2=\left[\frac{1}{\{e\}}\right]=[\alpha_1]=1$，$\alpha_2=\frac{1}{0.392205\cdots}$；

$a_3=[\alpha_2]=2$，$\alpha_3=\frac{1}{0.54972\cdots}$；

$a_4=[\alpha_3]=1$，$\alpha_4=\frac{1}{0.819107\cdots}$；

$a_5=[\alpha_4]=1$，$\alpha_5=\frac{1}{0.220837\cdots}$；

$\therefore\quad e=[2,\ 1,\ 2,\ 1,\ 1,\ \cdots]$。

$\frac{P_1}{Q_1}=2$，$\frac{P_2}{Q_2}=2+\frac{1}{1}=3$，$\frac{P_3}{Q_3}=2+\frac{1}{1}+\frac{1}{2}=\frac{8}{3}$，

$\frac{P_4}{Q_4}=\frac{a_4P_3+P_2}{a_4Q_3+Q_2}=\frac{11}{4}$，$\frac{P_5}{Q_5}=\frac{a_5P_4+P_3}{a_5Q_4+Q_3}=\frac{19}{7}$。

22　$\because x_1=-\frac{9}{2}+\frac{\sqrt{57}}{2}=-0.7250828\cdots$，

$$x_2=-\frac{9}{2}-\frac{\sqrt{57}}{2}=-8.2749172\cdots,$$

与上题同样的方法计算得

$x_1=[-1,\ 3,\dot{1},\ 1,\ 1,\ 3,\ 7,\ \dot{3}]\approx-0.7250$；

$x_2=[-9,\ 1,\ 2,\ \dot{1},\ 1,\ 1,\ 3,\ 7,\ \dot{3}]\approx-8.2750$。

注意：实际求连分数的过程中，不必把$\sqrt{57}$化成小数，而直接求出$[x_1]$，$[x_2]$等等来确定连分数的各项之值。

23　令$f(x)=x^3-x^2-2x+1=0$，而$f(2)=1$，$f(1)=-1$，$f(0)=1$，$f(-1)=1$，$f(-2)=-9$，故$f(x)=0$有三个实根，它们分别存在于：$2>x_1>1$；$1>x_2>0$；$-1>x_3>-2$。

今先求x_1，令$x=1+\frac{1}{y}$

$$f(x)=\left(\frac{1}{y}\right)^3+2\left(\frac{1}{y}\right)^2-\frac{1}{y}-1$$

	1	−1	−2	1
1	1	0	−2	−1
1	1	1	−1	
1	1	2		

$\therefore$　$g(y)=y^3+y^2-2y-1$。

由笛卡尔符号法则知道，$g(y)$有且只有一个正根，并且$g(1)=-1$，$g(2)=7$，令$y=1+\frac{1}{z}$，得

$$h(z)=z^3-3z^2-4z-1$$

而$h(4)=-1$，$h(5)=29$，令$z=4+\frac{1}{\omega}$，得

$$k(w)=w^3-20w^2-9w-1.$$

有根在（20，21）中

$\therefore$　$x_1=[1,\ 1,\ 4,\ 20,\ \cdots]$

q_s		1	1	4	20	…
P_s	1	1	2	9	182	…
Q_s	0	1	1	5	101	…

$\therefore$　$x_1\approx\frac{182}{101}\approx1.8019$。

同样方法，计算得

$x_2=[0,\ 2,\ 4,\ 20,\ \cdots]\approx0.4450$。

$x_3=[-2,\ 1,\ 3,\ 20,\ 2,\ \cdots]\approx-1.2469$。

24 (i)

	1	0	2	0	3
1	1	1	3	1	6

$\therefore\ \{1, 0, 2, 0, 3\} = 6$.

(ii) $\left\{1, \frac{1}{2}, \frac{1}{2}, 2\right\} = \left\{1, \frac{1}{2}\right\} \cdot \left\{\frac{1}{2}, 2\right\} + \{1\} \cdot \{2\}$

$= \frac{3}{2} \times 2 + 1 \times 2 = 5$.

(iii) $\{2, -2, 3, -3, 1, -4\} = \{2, -2, 3\}\{-3, 1, -4\}$
$+ \{2, -2\}\{1, -4\} = -7 \times 5 + (-3)(-3) = -26$.

(iv) $\{\alpha, \beta, \gamma, \delta\} = \{\alpha, \beta\}\{\gamma, \delta\} + \{\alpha\}\{\delta\} =$
$= (\alpha\beta + 1)(\gamma\delta + 1) + \alpha\delta = \alpha\beta\gamma\delta + \alpha\beta + \gamma\delta + \alpha\delta + 1$.

(v) $\left\{3, 0, \frac{1}{2}, 0, 0, 1\right\} = \{3, 0\}\left\{\frac{1}{2}, 0, 0, 1\right\}$

$+ \{3\} \times \{0, 0, 1\} = 1 \times \frac{3}{2} + 3 \times 1 = \frac{9}{2}$.

25 $\{1, 2, 1, 3, 2, 3, 2\} = \{1, 2, 1\}\{3, 2, 3, 2\} +$
$+ \{1, 2\}\{2, 3, 2\}$.

左边 = 268；右边 = $4 \times 55 + 3 \times 16 = 220 + 48 = 268$.

26 (i) 设 $\alpha = [\dot{2}, 4, 1, \dot{3}] = [2, 4, 1, 3, \alpha]$

$\therefore\quad \alpha = \dfrac{\alpha P_4 + P_3}{\alpha Q_4 + Q_3}$,

其中

q_i		2	4	1	3	…
P_s	1	2	9	11	42	…
Q_s	0	1	4	5	19	…

$\therefore$

即 $P_4 = 42$, $P_3 = 11$, $Q_4 = 19$, $Q_3 = 5$，故由（1）知 α 是下列方程的根：

$$19x^2 - 37x - 11 = 0。$$

(ii) 与(i)一样地，求得$P_4 = 81$，$P_3 = 13$，$Q_4 = 56$，$Q_3 = 9$，知连分数$[\dot{1}, 2, 4, \dot{6}]$是下列方程的根：

$$56x^2 - 72x - 13 = 0。$$

(iii) 因为

q_s		2	1	2	1	1	3	1	1	3	α_{6}
P_s	1	2	3	8	11	19	68	87	155	552	
Q_s	0	1	1	3	4	7	25	32	57	203	

$$\therefore \quad \alpha = \frac{68\alpha_6 + 19}{25\alpha_6 + 7} = \frac{552\alpha_6 + 155}{203\alpha_6 + 57},$$

$$\alpha_6 = \frac{-7\alpha + 19}{25\alpha - 68} = \frac{-57\alpha + 155}{203\alpha - 55} \Longrightarrow 2\alpha^2 - 15\alpha + 26 = 0,$$

即$[2, 1, 2, \dot{1}, 1, \dot{3}]$是$2x^2 - 15x + 26 = 0$的根。

(iv) 因为

q_s		4	1	1	2	1	1	8	1	1	2	1	1	8	α_7
P_s	1	4	5	9	23	32	55	472	527	999	2525	3524	6049	51916	
Q_s	0	1	1	2	5	7	12	103	115	218	551	769	1320	11329	

$$\therefore \quad \alpha = \frac{472\alpha_7 + 55}{103\alpha_7 + 12} = \frac{51916\alpha_7 + 6049}{11329\alpha_7 + 1320},$$

$$\alpha_7 = \frac{-12\alpha + 55}{103\alpha - 472} = \frac{-1320\alpha + 6049}{11329\alpha - 51916} \Longrightarrow \alpha^2 - 21 = 0,$$

即$[4, \dot{1}, 1, 2, 1, 1, \dot{8}]$是$x^2 - 21 = 0$的根。

27 $\because \quad \frac{61}{11} = [5, 1, 1, 5]$,

$\therefore\quad 61=\{5,\ 1\}^2+\{5\}^2=6^2+5^2;$

$\because\quad \frac{137}{37}=[3,\ 1,\ 2,\ 2,\ 1,\ 3],$

$\therefore\quad 137=\{3,\ 1,\ 2\}^2+\{3,\ 1\}^2=11^2+4^2$

28　设 $(a,\ b)=d$，对于任意整数 x，y，都有 $d\mid ax+by$，所以只需证明形如 $ax+by$ 的整数中，最小的一个正数就是 d。

若 a，b 中有一个是 0，则不等 0 的那个整数的绝对值，是形如 $ax+by$ 的数中最小的一个正数，显然它整除 $ax+by$。

由于 $(a,\ b)=(|a|,\ |b|)$，若 a，b 都不等于 0，可设 $a>b>0$，当

$$\frac{a}{b}=[q_1,\ q_2,\ \cdots,\ q_n]$$

时，由定理1·12知

$$d=(-1)^{n-1}\{q_1,\ \cdots,\ q_{n-1}\}b+(-1)^n\{q_2,\ \cdots,\ q_{n-1}\}a$$

即存在 $x_0=(-1)^n\{q_2,\ \cdots,\ q_{n-1}\}$，$y_0=(-1)^{n-1}\{q_1,\ \cdots,\ q_{n-1}\}$ 使得 $ax_0+by_0=d$，它是形如 $ax+by$ 的整数中最小的正数。事实上，否则，若 $0<ax_1+by_1<ax_0+by_0=d$，则 $d\mid a$，$d\mid b\Longrightarrow d\mid ax_1+by_1$ 这是不可能的。

29　由带余除法定理知，$\exists q$，r 之

$$a=bq+r,\quad 0\leqslant r<|b|$$

(i)　当 $r\leqslant\frac{|b|}{2}$ 时，取 $s=q$，$t=r$，即所求的二整数；

(ii)　当 $r>\frac{|b|}{2}$，若 $b>0$，则取 $s=q+1$，$t=r-b$；若 $b<0$，则取 $s=q-1$，$t=r+b$，这样的 s，t 即所求的二整数。

当 b 是奇数时，绝对值不大于 b 的余数是唯一的，所以 s，t 是唯一的；当 b 是偶数时，其余数允许是 $\frac{|b|}{2}$ 或 $-\frac{|b|}{2}$。故有时有二解。

30　当 $n=1$ 时，$f(x)=a_0x+a_1$，可取适当的整数 x_0，使 $a_0x_0+a_1=k$，$|k|>1$，则 $x=x_0+nk$ 时，$f(x)=(a_0n+1)k$，除 $a_0n+1=\pm 1$ 外都是合数。

今讨论$n>1$的情况，因为$a_0>0$，所以当$x_0=n\times\max(|a_1|,\cdots,|a_n|)=n\alpha$时，并且可取$\alpha>1$，则

$$a_0x_0^n=a_0n^n\alpha^n\geqslant n^n\alpha^n,$$

要证

$$f(x_0)=a_0(n\alpha)^n+a_1(n\alpha)^{n-1}+\cdots+a_{n-1}n\alpha+a_n>1$$

只要证

$$n^n\alpha^n>\alpha[(n\alpha)^{n-1}+\cdots+n\alpha+1]+1=\alpha\frac{n^n\alpha^n-1}{n\alpha-1}+1$$

$$\Longrightarrow n^n\alpha^n(n\alpha-\alpha-1)>n\alpha-\alpha-1$$

因为$n>1$，$\alpha>1$，所以上面不等式显然成立，因而$f(x_0)>1$。同样地，易得$f'(x_0)>0$。

令$f(x_0)=X$，则

$$f(x_0+Xt)=f(x_0)+f'(x_0)Xt+\frac{f''(x_0)}{2!}(Xt)^2+\cdots$$

$$=X(1+f'(x_0)t+\frac{f''(x_0)}{2!}Xt^2+\cdots)(t=1,\ 2,\ \cdots)$$

由于$x\geqslant x_0$时，$f(x)$是增函数，所以$f(x_0+Xt)>f(x_0)$，即$x=x_0+Xt$（$t=1,2,\cdots$）时，$f(x)$都是合数（X都是$f(x_0+Xt)$的一个真因数）。

31　由贾宪三角知$(a+b)^n$的展开式的各项系数，当$n=0,1,\cdots,8$时，依次是

1

1　1

1　2　1

1　3　3　1

1　4　6　4　1

1　5　10　10　5　1

1　6　15　20　15　6　1

1　7　21　35　35　21　7　1

1　8　28　56　70　56　28　8　1

所以当且仅当 $n=1$，3，7（$1=2^1-1$，$3=2^2-1$，$7=2^3-1$）时 $(a+b)^n$的系数都是奇数。一般地，

$$\because\quad \sum_{t=1}^{\infty}\left[\frac{n}{2^t}\right]\geqslant\sum_{t=1}^{\infty}\left(\left[\frac{h-r}{2^t}\right]+\left[\frac{r}{2^t}\right]\right),$$

所以只须证，当$n=2^k-1$时取等号；当$n\neq 2^k-1$时，取“>”号。即当且仅当$n=2^k-1$时（$a+b$）^{n}展开式的各项系数都是奇数。

若$n=2^k-1$时，则由函数$[x]$的性质(iv)得

$$\sum_{t=1}^{\infty}\left[\frac{n}{2^t}\right]=\sum_{t=1}^{\infty}\left[\frac{2^k-1}{2^t}\right]=(2^{k-1}-1)+(2^{k-2}-1)+\cdots+$$

$$+(2^2-1)+(2-1)$$

$$=2^k-1-k=2^k-(k+1).$$

令$\sum_{t=1}^{\infty}\left[\frac{n-r}{2^t}\right]+\sum_{t=1}^{\infty}\left[\frac{r}{2^t}\right]=T$，则

$$T=\sum_{t=1}^{\infty}\left(\left[\frac{2^k-r-1}{2^t}\right]+\left[\frac{r}{2^t}\right]\right)=\sum_{t=1}^{k-1}\left(2^{k-t}+\left[\frac{-(r+1)}{2^t}\right]\right.$$

$$\left.+\left[\frac{r}{2^t}\right]\right)$$

当$2^t\mid r+1$时，

$$\left[\frac{-(r+1)}{2^t}\right]=-\left[\frac{r+1}{2^t}\right],\quad\left[\frac{r}{2^t}\right]=\left[\frac{r+1}{2^t}\right]-1;$$

当$2^t\nmid r+1$时，

$$\left[\frac{-(r+1)}{2^t}\right]=-\left[\frac{r+1}{2^t}\right]-1,\quad\left[\frac{r}{2^t}\right]=\left[\frac{r+1}{2^t}\right].$$

$$\therefore\quad T=(2^{k-1}-1)+(2^{k-2}-1)+\cdots+(2-1)=\sum_{t=1}^{\infty}\left[\frac{n}{2^t}\right]$$

反之，当（$a+b$）^{n} 的系数全为奇数，即对于 任 意 $0\leqslant r\leqslant n$，都有

$$\sum_{t=1}^{\infty}\left[\frac{n}{2^t}\right]=\sum_{t=1}^{\infty}\left(\left[\frac{n-r}{2^t}\right]+\left[\frac{r}{2^t}\right]\right).$$

今用反证法证明之。由于当n为偶数时，$(a+b)^n$的展开式出现以n为系数的项，故不全为奇数，所以，如果n不是形如2^k-1的数，样末$n=2^k+s$，s是正奇数，且$s\leqslant 2^k-3$。又因为

$$\left[\frac{n}{2^t}\right]\geqslant\left[\frac{n-r}{2^t}\right]+\left[\frac{r}{2^t}\right]=\left[\frac{l2^t+s_t-r}{2^t}\right]+\left[\frac{r}{2^t}\right]$$

$$=l+\left[\frac{s_t-r}{2^t}\right]+\left[\frac{r}{2^t}\right],$$

其中$s_t<2^t<n$，并且s_t是奇数。可取适当的t和r，使得

$$s_t<r<2^t.$$

〔例如，取$t=k$时，$1\leqslant s_k=s\leqslant 2^k-3$（∵ $n=2^k+s\leqslant 2^k+2^k-3$）取$r=s+1$，就有$s<r<2^k$。〕那末$\left[\frac{s_t-r}{2^t}\right]=-1$，$\left[\frac{r}{2^t}\right]=0$，即$\left[\frac{n-r}{2^t}\right]+\left[\frac{r}{2^t}\right]=l-1$，而

$$\left[\frac{n}{2^t}\right]=\left[\frac{l2^t+s_t}{2^t}\right]=l>\left[\frac{n-r}{2^t}\right]+\left[\frac{r}{2^t}\right].$$

即$(a+b)^n$的系数不全为奇数。

32 (i) $\sum_{t=1}^{\infty}\left[\frac{30}{2^t}\right]=15+7+3+1=26$；

$\sum_{t=1}^{\infty}\left[\frac{30}{3^t}\right]=10+3+1=14$；

$\sum_{t=1}^{\infty}\left[\frac{30}{5^t}\right]=6+1=7$； $\sum_{t=1}^{\infty}\left[\frac{30}{7^t}\right]=4$；

$\left[\frac{30}{11}\right]=2$； $\left[\frac{30}{13}\right]=2$； $\left[\frac{30}{17}\right]=1$； $\left[\frac{30}{19}\right]=1$；

$\left[\frac{30}{23}\right]=1$； $\left[\frac{30}{29}\right]=1$。

$\therefore\quad 30! = 2^{26}\cdot3^{14}\cdot5^{7}\cdot7^{4}\cdot11^{2}\cdot13^{2}\cdot17\cdot19\cdot23\cdot29.$

(ii) $\sum_{t=1}^{\infty}\left[\frac{250}{3^t}\right] = 83+27+9+3+1=123$

$\sum_{t=1}^{\infty}\left[\frac{250}{7^t}\right] = 35+5=40;\qquad \sum_{t=1}^{\infty}\left[\frac{250}{11^t}\right] = 22+2=24;$

$\sum_{t=1}^{\infty}\left[\frac{250}{23^t}\right] = 10.$

所以250!中含有3^{123}，7^{40}，11^{24}，23^{10}的因子。

33 下面等号上面的注释是$[\alpha]$，$\{\alpha\}$的性质的番号。

(i) $[n\alpha] \overset{(i)}{=\!=} [n[\alpha]+n\{\alpha\}] \overset{(iv)}{=\!=} n[\alpha]+[n\{\alpha\}] = n[\alpha]+k$

$(0\leqslant k<n)$

右边$\overset{(i)}{=\!=} n[\alpha]+[\{\alpha\}]+\left[\{\alpha\}+\frac{1}{n}\right]+\cdots+\left[\{\alpha\}+\frac{n-1}{n}\right]$

$= n[\alpha]+0+\left[\frac{n\{\alpha\}+1}{n}\right]+\cdots+\left[\frac{n\{\alpha\}+n-1}{n}\right]$

$= n[\alpha]+\left[\frac{k+1+\{n\{\alpha\}\}}{n}\right]+\cdots+\left[\frac{k+n-1+\{n\{\alpha\}\}}{n}\right]$

$= n[\alpha]+k =$ 右边。

(ii) $[2\alpha]+[2\beta] \overset{(i)}{=\!=} [2[\alpha]+2\{\alpha\}]+[2[\beta]+2\{\beta\}]$

$\overset{(iv)}{=\!=} 2[\alpha]+2[\beta]+[2\{\alpha\}]+[2\{\beta\}];$

右边$\overset{(i)(iv)}{=\!=\!=} [\alpha]+[\beta]+[\alpha]+[\beta]+[\{\alpha\}+\{\beta\}]$

$= 2[\alpha]+2[\beta]+[\{\alpha\}+\{\beta\}].$

最后证明，$[2\{\alpha\}]+[2\{\beta\}]\geqslant[\{\alpha\}+\{\beta\}]$，

(a) 当$\{\alpha\}\geqslant0.5$，$\{\beta\}\geqslant0.5$时，$[2\{\alpha\}]+[2\{\beta\}]=2$，而$[\{\alpha\}+\{\beta\}]=1$，故该不等式成立；

(b) 当$\{\alpha\}\geqslant0.5$，$\{\beta\}<0.5$或$\{\beta\}\geqslant0.5$，$\{\alpha\}<0.5$时，$[2\{\alpha\}]+[2\{\beta\}]=1$，而$[\{\alpha\}+\{\beta\}]\leqslant1$，故该不等式成立。

(c) 当$\{\alpha\}<0.5$，$\{\beta\}<0.5$时，

$$[2\{\alpha\}]+[2\{\beta\}]=[\{\alpha\}+\{\beta\}]=0.$$

(iii) $$[\alpha-\beta]=[[\alpha]-[\beta]+\{\alpha\}-\{\beta\}]=\begin{cases}[\alpha]-[\beta], & \text{当}\{\alpha\}\geqslant\{\beta\},\\ [\alpha]-[\beta]-1, & \text{当}\{\alpha\}<\{\beta\}.\end{cases}$$

∴ $[\alpha]-[\beta]=[\alpha-\beta]$或者$[\alpha]-[\beta]=[\alpha-\beta]+1$.

34 (i) 在横坐标等于整数的直线上，恰好有$[f(x)]$个整点，在平面区域

$Q<x\leqslant R$，$0<y\leqslant f(x)$

（如图1的阴影部分，不包括虚线及x轴部分）内的整点，所以其整点个数是：

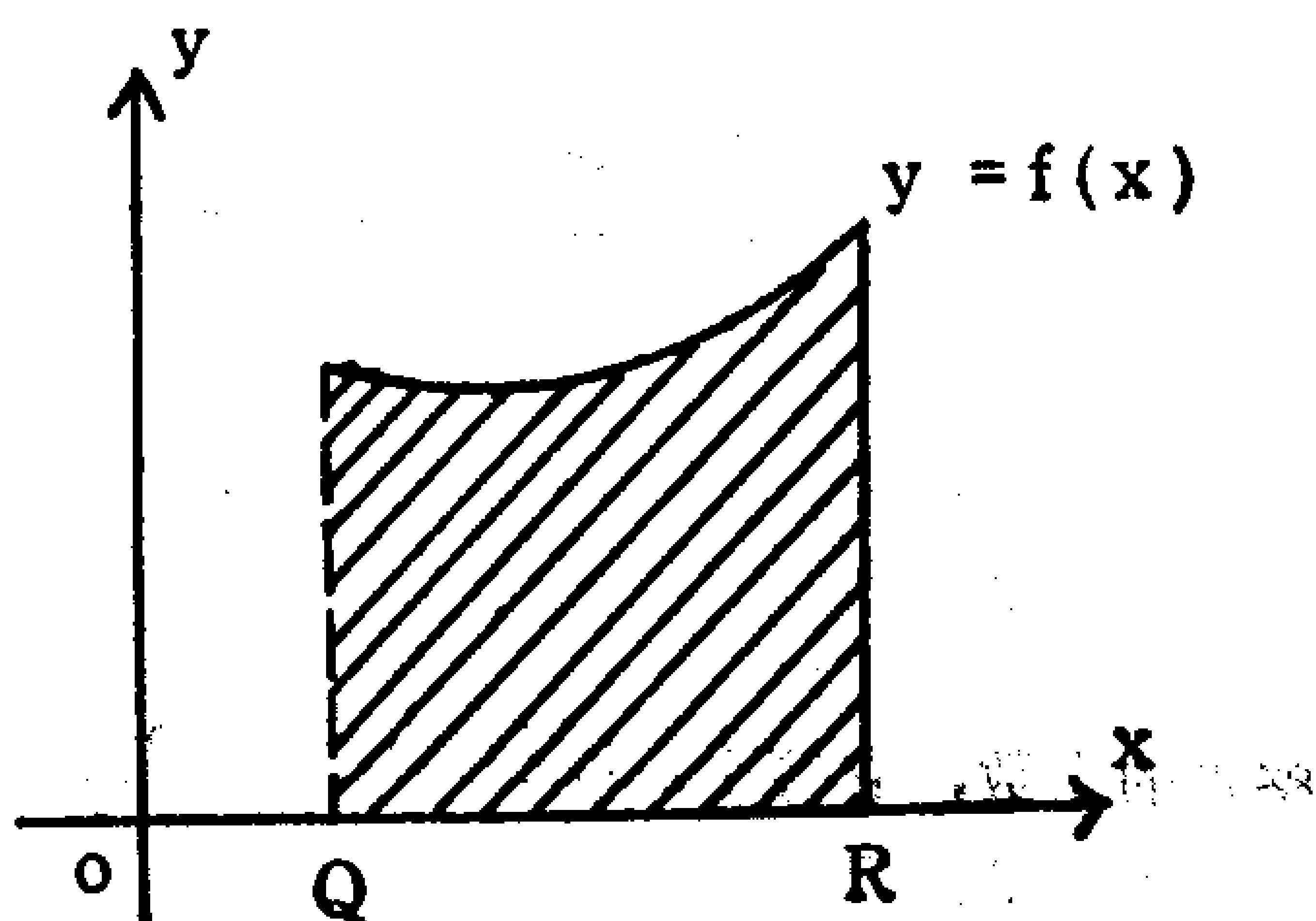


图 1

$$\sum_{Q<x\leqslant R}[f(x)],$$

其中x是整数。

(ii) 令$T_1=\sum\limits_{0<x<\frac{q}{2}}\left[\frac{p}{q}x\right]$，$T_2=\sum\limits_{0<y<\frac{p}{2}}\left[\frac{q}{p}y\right]$，

$T=\frac{p-1}{2}\cdot\frac{q-1}{2}$，其中x，y是整数，即$T_1$，$T_2$分别表示区域：

$0<x<\frac{q}{2}$，$0<y<\frac{p}{q}x$，

$0<y<\frac{p}{2}$，$0<x<\frac{q}{p}y$.

里的整点个数。即△OAC和△OAB内的整点个数（如图2，不包边界上的点）。因为p，q是互素的正奇数，所以在线段OA上除原点外无其他整点。$T=\frac{p-1}{2}\cdot\frac{q-1}{2}$表示矩形OBAC内(不包括边界)的

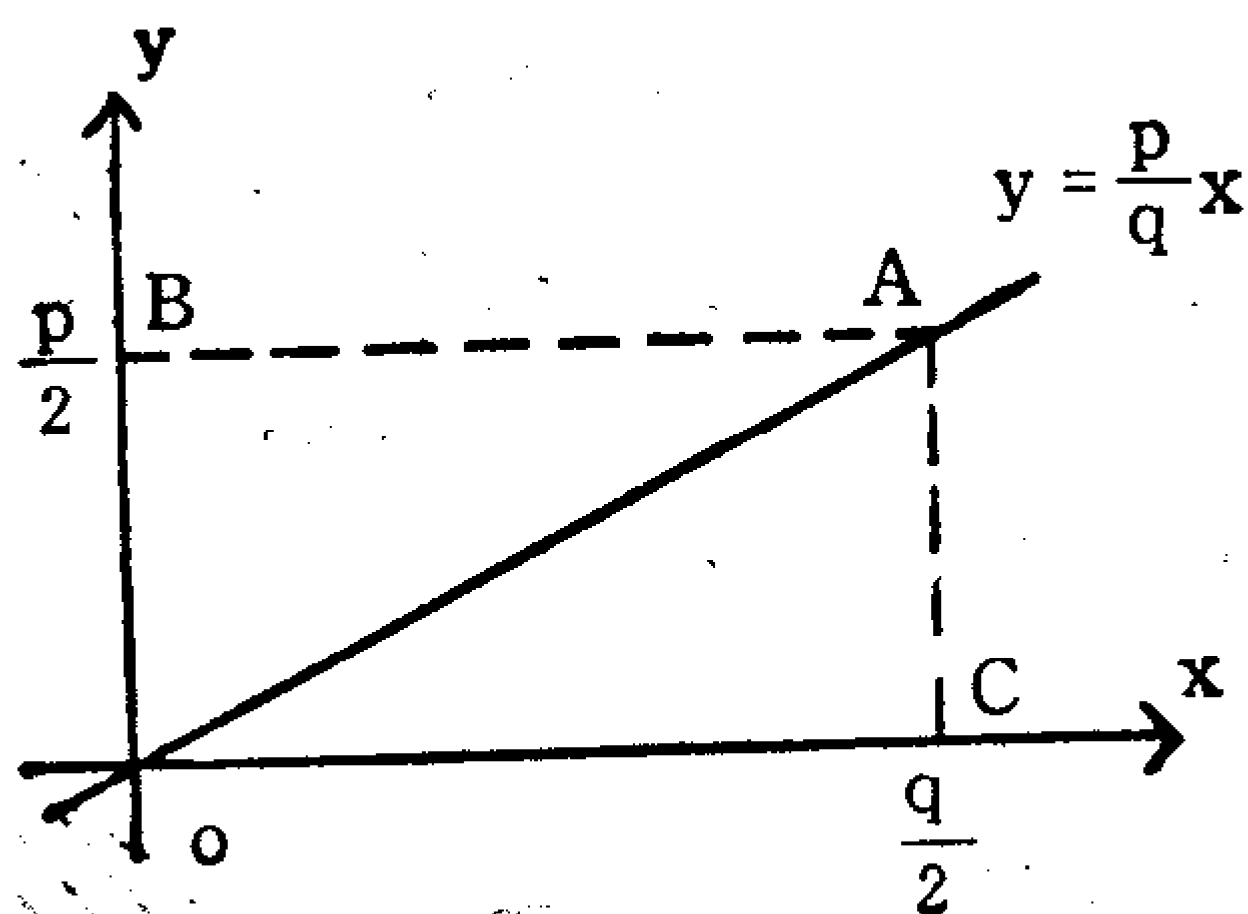


图 2

整点的个数。它等于△OAC和△OAB内整点个数之和。

∴　$T_1+T_2=T$。

(iii)　设T_1，T_2，T_3，T_4依次表示下列区域中的整点的个数：

$x=0$，$0<y\leqslant r$；$0<x\leqslant\frac{r}{\sqrt{2}}$，$0<y\leqslant\sqrt{r^2-x^2}$；

$0<y\leqslant\frac{r}{\sqrt{2}}$，$0<x\leqslant\sqrt{r^2-y^2}$；$0<x\leqslant\frac{r}{\sqrt{2}}$，$0<y\leqslant\frac{r}{\sqrt{2}}$。

如图 3，T_1是OB上的整点数（不包括原点）；T_2是区域ORPB内的整点数（不包括OR，OB上的点）；T_3是区域OAPQ内的整点数（不包括OA，OQ上的点）；T_4是区域ORPQ内的整点数（不包括OR，OQ上的点）。所以区域$x^2+y^2\leqslant r^2$内的整点数

$T=1+4(T_1+T_2+T_3-T_4)$，

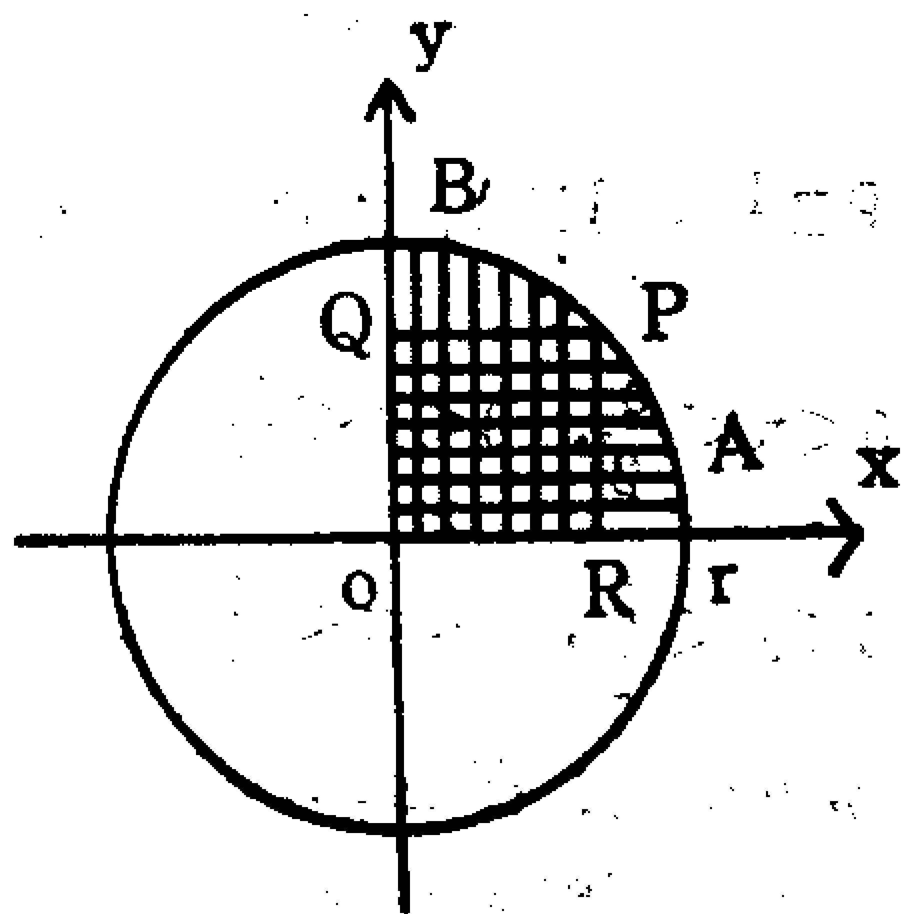


图 3

而$T_1=[r]$，$T_2=T_3=\sum\limits_{0<x\leqslant\frac{r}{\sqrt{2}}}[\sqrt{r^2-x^2}]$，$T_4=\left[\frac{r}{\sqrt{2}}\right]^2$.

$$\therefore\quad T=1+4[r]+8\sum_{0<x\leqslant\frac{r}{\sqrt{2}}}[\sqrt{r^2-x^2}]-4\left[\frac{r}{\sqrt{2}}\right]^2.$$

(iv) 设T_1，T_2，T_3依次表示下列区域内的整点个数：

$0<x\leqslant\sqrt{n}$，$0<y\leqslant\frac{n}{x}$；

$0<y\leqslant\sqrt{n}$，$0<x\leqslant\frac{n}{y}$；

$0<x\leqslant\sqrt{n}$，$0<y\leqslant\sqrt{n}$.

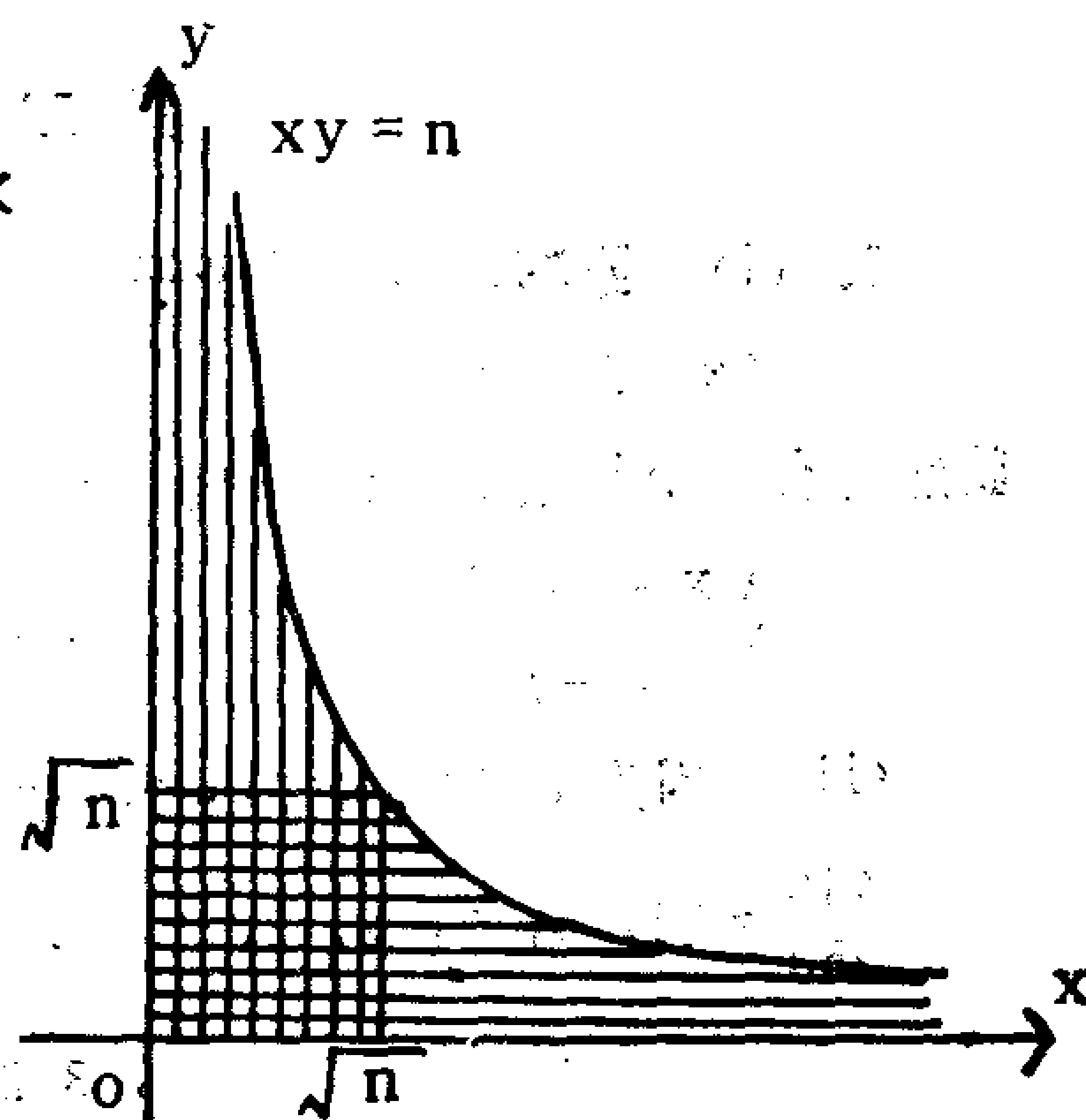


图 4

显然等边双曲线 $xy=n$ 在第一象限内的分支与x轴、y轴正向所围成的区域内的整点数 $T=T_1+T_2-T_3$，

而$T_1=T_2=\sum\limits_{0<x\leqslant\sqrt{n}}\left[\frac{n}{x}\right]$，$T_3=[\sqrt{n}]^2$

$$\therefore\quad T=2\sum_{0<x\leqslant n}\left[\frac{n}{x}\right]-[\sqrt{n}]^2.$$

35 当n是确定的正整数时，则右边多项式的项数有限，即

$n=a_0+a_1p+a_2p^2+\cdots+a_lp^l$，$0\leqslant a_i<p$

$$\therefore\quad h=\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots+\left[\frac{n}{p^l}\right]$$

$$=(a_1+a_2p+\cdots+a_lp^{l-1})+(a_2+\cdots+a_lp^{l-2})+\cdots+a_l$$

$$=a_1+a_2(p+1)+a_3(p^2+p+1)+\cdots+a_l(p^{l-1}+p^{l-2}+\cdots+1)$$

而

$$\frac{n-s_n}{p-1}=\frac{1}{p-1}[a_1(p-1)+a_2(p^2-1)+a_3(p^3-1)+\cdots+$$

$+a_l(p^l-1)]$

$=a_1+a_2(p+1)+a_3(p^2+p+1)+\cdots+a_l(p^{l-1}+p^{l-2}$

$+\cdots+1)$。

$\therefore\quad h=\dfrac{n-s_a}{p-1}$。

第 二 章

1. (i) 原不定方程等价于

$3x+5y=20$,

显然它有一个整数解：$x_0=10$，$y_0=-2$，故一般解是：

$$\begin{cases}x=10+5t,\\ y=-2-3t.\end{cases}\quad (t=0,\ \pm1,\ \pm2,\ \cdots).$$

(ii) 因为 $(253, 449)=1$，故该不定方程有解．而

$\dfrac{449}{253}=[1,\ 1,\ 3,\ 2,\ 3,\ 1,\ 1,\ 3]$,

$$\frac{\begin{matrix}1 & 1 & 3 & 2 & 3 & 1 & 1\end{matrix}}{\begin{matrix}1 & 1 & 2 & 7 & 16 & 55 & 71 & 126\end{matrix}}.$$

$\therefore\quad y_0=(-1)^8(-71)=-71$，$x_0=(-1)^{8-1}126=-126$,

故一般解是：$\begin{cases}x=-126+449t,\\ y=-71+253t.\end{cases}\quad (t=0,\ \pm1,\ \pm2,\ \cdots)$

(iii) 先求 $53x+47y=1$的解．

$\dfrac{53}{47}=[1,\ 7,\ 1,\ 5]$，$\dfrac{\begin{matrix}1 & 7 & 1\end{matrix}}{\begin{matrix}1 & 1 & 8 & 9\end{matrix}}\Longrightarrow x_0'=(-1)^4 8=8$,

$y_0'=(-1)^3 9=-9$。

$\therefore\quad x_0=11\times8=88$，$y_0=11\times(-9)=-99$,

是原不定方程的一个解．其一般解是：

$$\begin{cases}x=88+47t,\\ y=-99-53t;\end{cases}\quad 或\begin{cases}x=-6+47t,\\ y=7-53t.\end{cases}\quad (t=0,\ \pm1,\ \cdots).$$

(iv) $\because\quad \dfrac{\{\alpha,\ \beta,\ \gamma,\ \delta\}}{\{\beta,\ \gamma,\ \delta\}}=[\alpha,\ \beta,\ \gamma,\ \delta]$,

$\therefore\quad x_0=(-1)^4\{\beta,\ \gamma\}=\{\beta,\ \gamma\},\quad -y_0=(-1)^3\{\alpha,\ \beta,\ \gamma\}$
$=-\{\alpha,\ \beta,\ \gamma\}$。

故一般解是：$\begin{cases} x=\{\beta,\ \gamma\}+\{\beta,\ \gamma,\ \delta\}t, \\ y=-\{\alpha,\beta,\gamma\}+\{\alpha,\ \beta,\ \gamma,\ \delta\}t. \end{cases}\quad (t=0,\ \pm 1,\cdots)$

(v)　$(6,\ 3)=3$，先解 $6x+3z=3t$，即 $2x+z=t$，解得

$$\begin{cases} x=t-u, \\ z=-t+2u. \end{cases}\quad (u=0,\ \pm 1,\ \cdots).$$

次解　$3t-5y=1$，解得

$$\begin{cases} t=2+5v, \\ y=1+3v, \end{cases}\quad (v=0,\ \pm 1,\ \cdots).$$

$$\therefore\quad \begin{cases} x=2-u+5v, \\ y=1-3v, \\ z=-2+2u-5v. \end{cases}\quad (u,\ v=0,\ \pm 1,\ \cdots)$$

注意：亦可把 x看作自由未知量，令$x=u$，解二元不定方程 $-5y+3z=1-6u$，得

$$\begin{cases} x=u, \\ y=1-3v,\quad (u,\ v=0,\ \pm 1,\ \cdots) \\ z=2-2u-5v. \end{cases}$$

(vi)　先解 $5x_1+4x_2=t$，解得

$$\begin{cases} x_1=t-4u, \\ x_2=-t+5u. \end{cases}\quad (u=0,\ \pm 1,\ \cdots).$$

次解 $t-7x_3=t'$，解得

$$\begin{cases} t=8t'+7v, \\ x_3=t'+v. \end{cases}\quad (v=0,\ \pm 1,\ \cdots).$$

最后解 $t'-3x_4=5$，解得

$$\begin{cases} t'=-1+3w, \\ x_4=-2+w. \end{cases}\quad (w=0,\ \pm 1,\ \cdots)$$

$$\therefore\begin{cases} x=-8-4u+7v+24w, \\ x_2=8+5u-7v-24w, \\ x_3=-1+v+3w, \\ x_4=-2+w. \end{cases} \quad (u,\ v,\ w=0,\ \pm1,\ \cdots).$$

2。依题意即求 $7x+11y=100$的正整数解，解得：$x_0=8$，$y_0=4$，一般解是：

$$\begin{cases} x=8-11t, \\ y=4+7t. \end{cases} \quad (t=0,\ \pm1,\ \cdots)$$

但除 $t=0$外无其他正整数解，故有且只有

$$100=56+44.$$

3。$2\times(1)+(2)$得，$13x+13y=52$，即

$$x+y=4, \tag{3}$$

解得

$$\begin{cases} x=1-t, \\ y=3+t. \end{cases} \quad (t=0,\ \pm1,\ \cdots)$$

当且仅当 $t=0$，-1，-2时，(3)有正整数解(1，3)，(2，2)(3，1)，而依次把它代入(1)得：$z=-1$，0，1，前两个非正整解，故它的正整数解，只有一个，即 $x=3$，$y=1$，$z=1$。

4. 设一分、二分、五分分别取 x、y、z 枚付款，依题意有

$$\begin{cases} x+y+z=10, & (1) \\ x+2y+5z=18. & (2) \end{cases}$$

(2)－(1)得，$y+4z=8$。 (3)

(3)有且只有非负整数解：

$$\begin{cases} y=0, \\ z=2; \end{cases} \quad \begin{cases} y=4, \\ z=1; \end{cases} \quad \begin{cases} y=8, \\ z=0. \end{cases}$$

代入(1)得

$$\begin{cases} x=8, \\ y=0, \\ z=2; \end{cases} \quad \begin{cases} x=5, \\ y=4, \\ z=1; \end{cases} \quad \begin{cases} x=2, \\ y=8, \\ z=0. \end{cases}$$

5. 即求$72x+30y=750$的非负整数解，而$(72, 30)=6$，$6|750$，故该不定方程有解，且它等价于

$$12x+5y=125.$$

解得(0, 25)，(5, 13)，(10, 1)三非负整数解。

即有三种裁剪方法，大人和小孩各剪0，25；5，13；10，1件。

6. ∵ $N=[N]+\{N\}$，$N_1=[N_1]+\{N_1\}$，$N_2=[N_2]+\{N_2\}$，

∴ $[N]+\{N\}=[N_1]+[N_2]+\{N_1\}+\{N_2\}$

又因 $\{N_1\}+\{N_2\}\geqslant\{N_1+N_2\}=\{N\}$，

∴ $\{N_1\}+\{N_2\}=\begin{cases}\{N\},\\ \{N\}+1\end{cases}\Longrightarrow[N]+\{N\}=[N_1]+[N_2]+$

$$+\begin{cases}\{N\},\\ \{N\}+1.\end{cases}$$

∴ $[N_1]+[N_2]=\begin{cases}[N],\\ [N]-1.\end{cases}$

7. 当$N<0$时，(1)没有非负整数解，而$[\frac{N}{ab}]+1\leqslant0$，故命题正确；当$N=0$时，(1)有且只有一个非负整数解(0, 0)，而$[\frac{N}{ab}]=0$，$[\frac{N}{ab}]+1=1$，故命题亦真。下面研究$N>0$的情况。

因为$(a, b)=1$，所以(1)有整数解(x_0, y_0)，$y_0=(-1)^{n-1}\{q_1, \cdots, q_{n-1}\}N$，$x_0=(-1)^n\{q_2, \cdots, q_{n-1}\}N$，其中$\frac{a}{b}=[q_1, q_2, \cdots, q_n]$。由于$a>b>0$故$x_0$，$y_0$必一正一负。可设$x_0>0$，$y_0\leqslant0$，(1)的一般解是：

$$\begin{cases}x=x_0-bt,\\ y=y_0+at.\end{cases}\quad(t=0, \pm1, \cdots)$$

要求$x_0-bt\geqslant0$，$y_0+at\geqslant0\Longrightarrow\frac{x_0}{b}\geqslant t\geqslant-\frac{y_0}{a}\geqslant0$，仅当$-\frac{y_0}{a}$是整数时，才能取$t=[-\frac{y_0}{a}]$，否则$t>[-\frac{y_0}{a}]$。故这个不等式$t$的整数解个数T是：

当$\frac{y_0}{a}$是整数时，$T=[\frac{x_0}{b}]-[-\frac{y_0}{a}]+1\overset{(v)}{=\!=}[\frac{x_0}{b}]+[\frac{y_0}{a}]$

$+1$ 由上题知，$[\frac{N}{ab}]=[\frac{x_0}{b}]+[\frac{y_0}{a}] \Longrightarrow T=[\frac{N}{ab}]+1$。

当 $\frac{y_0}{a}$ 不是整数时，$T=[\frac{x_0}{b}]-[\frac{-y_0}{a}] \xlongequal{(v)} [\frac{x_0}{b}]+[\frac{y_0}{a}]$

$$+1 \text{由上题知，} [\frac{N}{ab}]=\begin{cases}[\frac{x_0}{b}]+[\frac{y_0}{a}], \\ [\frac{x_0}{b}]+[\frac{y_0}{a}]+1.\end{cases}$$

$$\therefore \qquad T=\begin{cases}[\frac{N}{ab}], \\ [\frac{N}{ab}]+1.\end{cases}$$

8. 先证后一点：当 $N=ab-a-b$ 时，（2）若有非负整数解 (x_0, y_0)，则 $ax_0+by_0=ab-a-b \Longrightarrow a(x_0+1)+b(y_0+1)=ab$，$x_0+1>0$，$y_0+1>0 \Longrightarrow b|x_0+1$，$a|y_0+1 \Longrightarrow x_0+1=bk$，$y_0+1=ah$，$k\geqslant 1$，$h\geqslant 1 \Longrightarrow ab(k+h)=ab$，$k+h\geqslant 2$。这是不可能的。

次证，当 $N>ab-a-b$ 时，因 $(a, b)=1$，故原同余式有整数解 (x_0, y_0)，一般解是：

$$\begin{cases}x=x_0-bt, \\ y=y_0+at.\end{cases} \quad (t=0, \ \pm 1, \ \cdots)$$

要求 $x_0-bt\geqslant 0$，$y_0+at\geqslant 0 \Longrightarrow -\frac{y_0}{a}\leqslant t\leqslant \frac{x_0}{b}$。今证明存在满足这个不等式的整数 $t=t_0$。

可取 t_0 使 $x_0=bt_0+r(0\leqslant r<b)$，于是对于这个 t_0 有，$x-bt_0=r\leqslant b-1 \Longrightarrow t_0\geqslant \frac{x-b+1}{b}$。而

$$y_0+at_0\geqslant y_0+\frac{a}{b}(x_0-b+1)=\frac{1}{b}(by_0+ax_0-ab+a)$$

$$=\frac{1}{b}(N-ab+a)>\frac{1}{b}(ab-a-b-ab+a)=-1,$$

$\therefore \quad y_0+at_0\geqslant 0 \Longrightarrow t_0\geqslant -\frac{y_0}{a}$.

这就证明了，当 $N>ab-a-b$ 时，（2）有非负整数解。

9. 因为$60=2^2\times3\times5$，所以要把$\frac{17}{60}$分成三个分母两两互素的分数之和，其分母可分别为4，3，5，分子为下列不定方程的整数解：

$$15x+20y+12z=17,$$

先求 $15x+20y=5t$，即 $3x+4y=t$的解，

$$\begin{cases}x=-t-4u,\\y=t+3u.\end{cases}\quad(u=0,\ \pm1,\ \cdots)$$

次求 $5t+12z=17$的解，

$$\begin{cases}t=1-12v,\\z=1+5v.\end{cases}\quad(v=0,\ \pm1,\ \cdots).$$

$$\therefore\quad\begin{cases}x=-1-4u+12v,\\y=1+3u-12v,\quad(u,\ v=0,\ \pm1,\ \cdots)\\z=1+5v.\end{cases}$$

由于对任意整数u，v，$(x,\ 4)=1$，$(y,\ 3)=1$，$(z,\ 5)=1$，故有无穷多个这样的既约分数之和，如，$u=v=0$时，$\frac{17}{60}=-\frac{1}{4}+\frac{1}{3}+\frac{1}{5}$；$u=v=1$时，$\frac{17}{60}=\frac{7}{4}-\frac{8}{3}+\frac{6}{5}$；$u=-2$，$v=0$时，$\frac{17}{60}=\frac{7}{4}-\frac{5}{3}+\frac{1}{5}$等等。

10. 设大和尚x个，小和尚y个，则

$$\begin{cases}x+y=100,\\3x+\frac{1}{3}y=100.\end{cases}$$

解得 $x=25$，$y=75$。

改后的情况，是求下列不定方程的非负整数解：

$$9x+y=300.$$

其非负整数解共有$\left[\frac{300}{9}\right]+1=33+1=34$个，是

$$\begin{cases}x=25-t,\\y=75+9t.\end{cases}\quad(t=-8,\ -7,\ \cdots,\ -1,\ 0,\ 1,\ \cdots,\ 25).$$

11. 设有布 x匹，共销（$10y+5.2$）元，即

$$253x-100y=52.$$

解得 $\begin{cases} x=84+100t, \\ y=212+253t. \end{cases}$ （$t=0, \pm1, \pm2, \cdots$）

由于匹数小于100，故只有 $x=84$（匹），$y=212$（10元）。

12. 只要证：

$$[(2n^2-3n)^2-(2n^2+n)^2]+[(2n^2-3n-1)^2-(2n^2+n+1)^2]+\cdots+[(2n^2+2n+1)^2-(2n^2+2n-1)^2]=4n^2(n+1)^2 \quad (1)$$

即可。（1）的

$$左边=2n(4n^2+4n)+(2n-2)(4n^2+4n)+\cdots+2(4n^2+4n)$$

$$=2\cdot\frac{n(n+1)}{2}(4n^2+4n)=右边。$$

13. 由定理2·3知道（1）的解是

$x=2cd$，$y=c^2-d^2$，$z^2=c^2+d^2$，$c>d>0$，$(c, d)=1$，c，d一奇一偶。其中 $c=2ab$，$d=a^2-b^2$，$z=a^2+b^2$，$a>b>0$，$(a, b)=1$，a，b一奇一偶，所以

$x=4ab(a^2-b^2)$，$y=|a^4+b^4-6a^2b^2|$，$z=a^2+b^2$，

是（1）的正整数解（$x>0$，$y>0$，$z>0$，$(x, y)=1$，$2|x$）。且a^2+b^2是奇数。

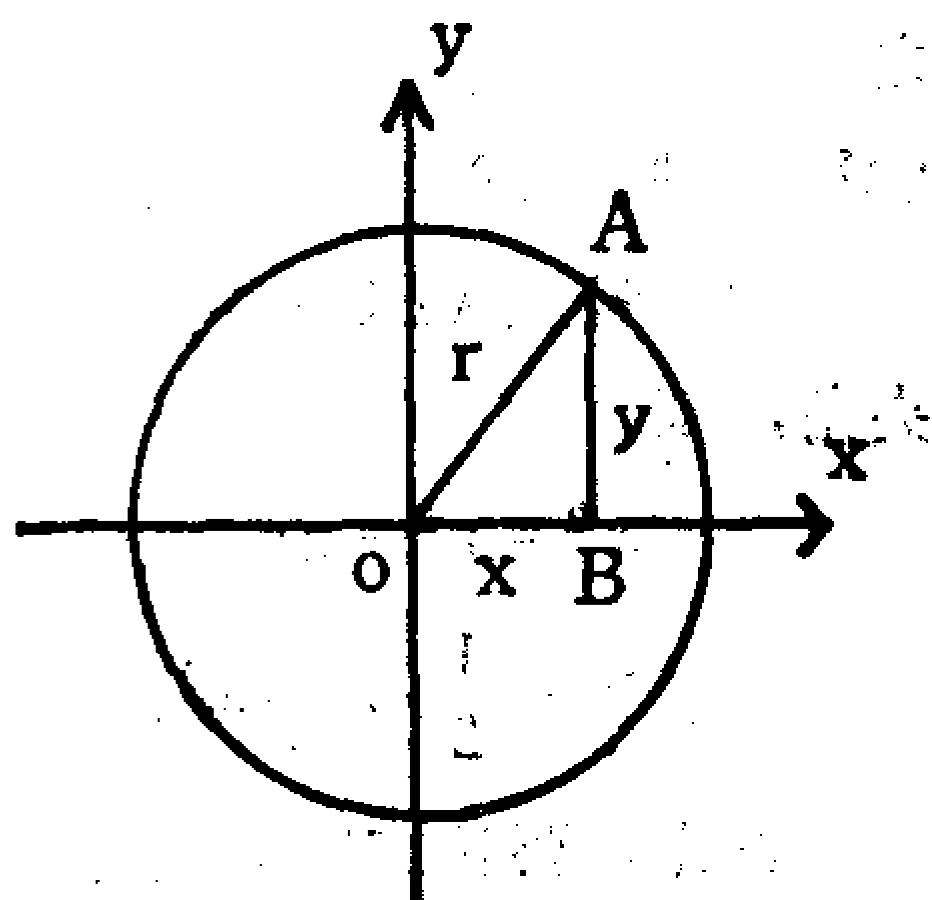
（1）的整数解有：$(0, 0, 0)$，$(0, \pm a^2, \pm a)$，$(\pm a^2, 0, \pm a)$，$(\pm 4ab(a^2-b^2), \pm(a^4+b^4-6a^2b^2), \pm(a^2+b^2))$，$(\pm(a^4+b^4-6a^2b^2), \pm 4ab(a^2-b^2), \pm(a^2+b^2))$，其中正负号可任意选取。

14. 由定理2·3及其引理2，可得

$x^2=2cd$，$y=|c^2-d^2|$，$z=c^2+d^2$，$c>0$，$d>0$，$(c, d)=1$，$2|c$。令$2c=a_1^2$，$d=b_1^2$，则 $a_1=2a$，$b_1=b$，得

$x=2ab$，$y=|4a^4-b^4|$，$z=4a^4+b^4$，$a>0$，$b>0$，$(a, b)=1$，a，b一奇一偶是（1）的解。今证明$2\nmid b$，因若$2|b$，则 x，y，z 都是偶数，这与$(x, y)=1$矛盾，故$2\nmid b$。

15. 设直角三角形OAB的斜边OA = r = 1，直角边OB = x，BA = y（如右图）．则$\sin\theta = y$，$\cos\theta = x$，要求x，y都是有理数，即单位圆上的有理点。由定理2·3的系知道一切如下的点：



$$\left(\pm\frac{2ab}{a^2+b^2},\ \pm\frac{a^2-b^2}{a^2+b^2}\right),$$

$$\left(\pm\frac{a^2-b^2}{a^2+b^2},\ \pm\frac{2ab}{a^2+b^2}\right)$$

都是有理点，其中a，b不全为零，正负号可以任意选取，所以当

$$\theta = \arcsin\left(\pm\frac{2ab}{a^2+b^2}\right)\text{或}\theta = \arcsin\left(\pm\frac{a^2-b^2}{a^2+b^2}\right)$$

时$\sin\theta$和$\cos\theta$都是有理数。

16. 显然x，y是正整数，把x的值代入（α）的左边，得

$$x^2+(x+1)^2 = 2x^2+2x+1 = \frac{1}{8}[(1+\sqrt{2})^{2n+1}+(1-\sqrt{2})^{2n+1}-2]^2 + \frac{1}{2}[(1+\sqrt{2})^{2n+1}+(1-\sqrt{2})^{2n+1}-2]+1 = \frac{1}{8}\{[(1+\sqrt{2})^{2n+1}-(1-\sqrt{2})^{2n+1}]+2[(1-\sqrt{2})^{2n+1}-1]\}^2 + \frac{1}{2}\{[(1+\sqrt{2})^{2n+1}-(1-\sqrt{2})^{2n+1}]+2[(1-\sqrt{2})^{2n+1}-1]\}+1 = \frac{1}{8}\{2\sqrt{2}y+2[(1-\sqrt{2})^{2n+1}-1]\}^2+[\sqrt{2}y+(1-\sqrt{2})^{2n+1}-1]+1 = y^2+\sqrt{2}y[(1-\sqrt{2})^{2n+1}-1]+\frac{1}{2}[(1-\sqrt{2})^{2n+1}-1]^2+\sqrt{2}y+(1-\sqrt{2})^{2n+1} = y^2+\sqrt{2}y(1-\sqrt{2})^{2n+1}+\frac{1}{2}(1-\sqrt{2})^{4n+2}+\frac{1}{2} = y^2+\frac{1}{2}[(1+\sqrt{2})^{2n+1}-(1-\sqrt{2})^{2n+1}](1-\sqrt{2})^{2n+1}+\frac{1}{2}(1-\sqrt{2})^{4n+2}+\frac{1}{2} = y^2+\frac{1}{2}(1-\sqrt{2})^{2n+1}(1+\sqrt{2})^{2n+1}+\frac{1}{2} = y^2.$$

实际上，这里已包括(α)的一切解了，不过我们没有证明(α)再

无其它正整数解。此题给出了相邻二正整数作为直角三角形二直角边之长的一切可能性。如，当 $n=1$时，即$3^2+4^2=5^2$；$n=2$时，即$20^2+21^2=29^2$；$n=3$时，即$119^2+120^2=169^2$等等。

17. 设△ABC的三边长分别为 x，y，z，θ为长 y，z 的两边的夹角，则

$$x^2=y^2+z^2-2yz\cos\theta,$$

$$S=\frac{1}{2}yz\sin\theta.$$

首先，要按15题的条件，给出 $\cos\theta$ 和 $\sin\theta$ 同为有理数的 θ，但应把 $\theta=0°$和$\theta=180°$除外。

令

$$\cos\theta=\frac{c}{d},\ d>|c|\Longrightarrow\sin\theta=\sqrt{1-\cos^2\theta}=\frac{\sqrt{d^2-c^2}}{|c|}$$

$\Longrightarrow$要求 $d^2-c^2=f^2$ 有解$\Longrightarrow$要求 $d^2=c^2+f^2$ 有解。

而 $c=2ab$，$f=a^2-b^2$，$d=a^2+b^2$ 或者 $c=a^2-b^2$，$f=2ab$，$d=a^2+b^2$ 是它的解，也就是

$$\frac{c}{d}=\pm\frac{2ab}{a^2+b^2}\text{或}\frac{c}{d}=\pm\frac{a^2-b^2}{a^2+b^2}$$

其中 a，b 是任意不全为 0 的整数（这里不要求 $(a,b)=1$），并且 $\frac{c}{d}\neq\pm1$。

当 $d^2-c^2=f^2(\frac{c}{d}\neq\pm1)$时，要求 $x^2=y^2+z^2-2yz\frac{c}{d}$ 的右边是完全平方，则

$$z=\frac{d}{c}y\Longrightarrow x^2=y^2+(\frac{d}{c}y)^2-2y^2=\left(\frac{d^2-c^2}{c^2}\right)y^2$$

$$=\left(\frac{f}{c}y\right)^2.$$

否则，

$$z=\frac{e}{g}y\Longrightarrow x^2=y^2(1+\frac{e^2}{g^2}-2\frac{ec}{gd})=\frac{g^2+e^2-2ge\frac{c}{d}}{g^2}y^2$$又恢复

到要求 $g^2+e^2-2ge\frac{c}{d}$ 是完全平方，当 $e=\frac{d}{c}g$， 即 $z=\frac{d}{c}y$ 时，它是完全平方。否则，又重复上面的结果，所以仅当

$$z=\frac{d}{c}y,\quad x=\frac{f}{c}y=\frac{\sqrt{d^2-c^2}}{c}y,$$

y 为任意有理数时，x，y，z 都是有理数。即

当 $c\neq 0$时，即 $a\neq\pm b$ 或 $a\neq 0$，$b\neq 0$时，

$$z=\frac{d}{c}y,\quad x=\pm\frac{\sqrt{d^2-c^2}}{c}y,\ y\text{ 是任意有理数。}$$

当 $c=0$时，即$x^2=y^2+z^2$ 的一切有理数解。

上述的一切 x，y，z 为边长的三角形，其面积也都是有理数。

18．把(α)的两边平方得

$$x^8-8x^4y^4+16y^8=z^4\Longrightarrow z^4+(2xy)^4=(x^4+4y^4)^2 \qquad (\beta)$$

由定理2·6知(β)无整数解。所以(α)亦无整数解。事实上，若(α)有整数解(x_0, y_0, z_0)，则$(z_0, 2x_0y_0, x_0^4+4y_0^4)$是$(\beta)$的整数解，这是不可能的。

19．若$(x, y)=(2ab, a^2-b^2)=d>1$，则

(i) 若$d=2t$，则$2|a$ 或$2|b\Longrightarrow 2|a$ 且$2|b$，这与$(a, b)=1$矛盾。

(ii) 若$d=2t+1=pq,(p,q)=1$，$p|a$，$q|b\Longrightarrow a=kp$，$b=hq$，$a^2-b^2=k^2p^2-h^2q^2=sd=spq\Longrightarrow pq|a^2$，$pq|b^2$，这与$(a, b)=1$矛盾

$\therefore$ $(x, y)=1\Longrightarrow(x, y, z)=1$。

20．仿照定理2·6的证法，亦用费马的无穷递降法。

若(1)有正整数解，则一定有一个 z 值最小的解，即存在一个最小的正整数 u，使得

$$x^4+4y^4=u^2,\quad x>0,\ y>0,\ u>0 \qquad (2)$$

有解。这时$(x, y)=1$，$(x, 2)=1$，否则，就有$(x, y)>1$，或$(x, 2)=2$，有

$$\left(\frac{x}{(x,y)}\right)^4+4\left(\frac{y}{(x,y)}\right)^4=\left(\frac{u}{(x,y)^2}\right)^2\Longrightarrow 0<\frac{u}{(x,y)^2}<u;$$

或，令 $x=2x'$，得

$$4x'^4+y^4=\left(\frac{u}{2}\right)^2\Longrightarrow 0<\frac{u}{2}<u,$$

都与 u 的最小性矛盾．把（2）写成

$$(x^2)^2+(2y^2)^2=u^2 \qquad (2)'$$

由定理2·3，得

$(2y)^2=2ab$，$x^2=a^2-b^2$，$u=a^2+b^2$，$a>b>0$，$(a,b)=1$，（3）

且 a，b 一奇一偶（否则 x，u 都是偶数，这是不可能的）．所以 $2|y$，$2\nmid x$ 且必然 $4|b$，$2\nmid a$．否则 $a=2a_1$，$b=2b_1+1\Longrightarrow x^2=4(a_1^2-b_1^2-b_1)-1$；又因 $x=2x_1+1\Longrightarrow x^2=4(x_1^2+x_1)+1$，这是不可能的。

于是可设 $b=4c$，得

$$\left(\frac{y}{2}\right)^2=ac,\ (a,c)=1$$

由定理2·3前面的引理，得

$a=d^2$，$c=f^2$，$d>0$，$f>0$，$(d,f)=1$．

代入（3）得

$x^2=d^4-16f^4\Longrightarrow(4f^2)^2+x^2=(d^2)^2$，

且 $(4f^2,x)|d^2$，$(4f^2,d^2)|x\Longrightarrow(4f^2,x)|(4f^2,d^2)$ 且 $(4f^2,d^2)|(4f^2,x)\Longrightarrow(4f^2,x)=(4f^2,d^2)=(b,a)=1$．$4f^2>0$，$x>0$．

由定理2·3得到 $(4f^2)^2+x^2=(d^2)^2$ 的整数解

$4f^2=2lm$，$x^2=l^2-m^2$，$d^2=l^2+m^2$，$l>m>0$，$(l,m)=1$，其中 m 是偶数，设 $m=2m_1$，得

$f^2=lm_1$．

由定理2·3前面的引理 2，得

$l=r^2$，$m_1=s^2$，$m=2s^2\Longrightarrow r^4+4s^4=d^2$．

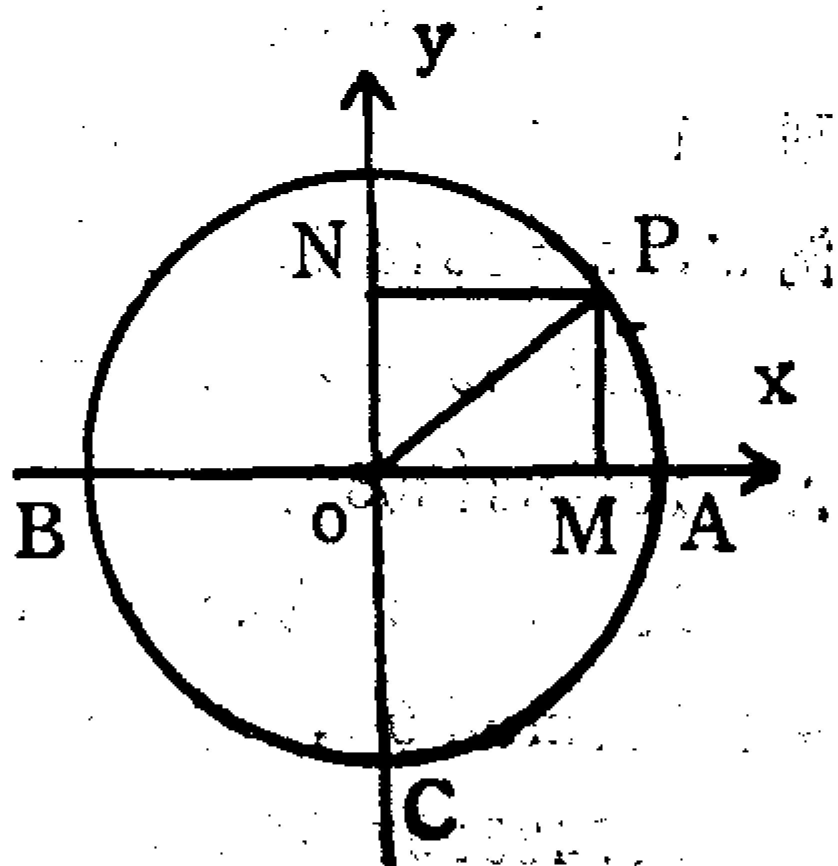
而 $u=a^2+b^2>a=d^2$，这与 u 的最小性矛盾，所以(1)无正整数解。

21．(1)的两边平方整理得

$$z^4+4(xy)^4=(x^4+y^4)^2. \tag{2}$$

若(2)有正整数解(x_0, y_0, z_0)，则前题的 $x=z_0$，$y=x_0y_0$，$z=x_0^4+y_0^4$就是$x^4+4y^4=z^2$的正整数解，这是不可能的。所以(1)无解。

22 此题证法有多种，今用最初等的方法证明于下。



因为 r 是奇数，且

$$u^2+v^2=r^2 \tag{1}$$

所以 u，v 必一奇一偶。

(i) 设 u 为偶数，由题意得

$u=2^m \Longrightarrow (r+u)(r-u)=v^2=q^{2n}$（q 是奇素数）$\Longrightarrow r+u=q^\alpha$，$r-u=q^\beta$，$\alpha>\beta \Longrightarrow 2u=q^\beta(q^{\alpha-\beta}-1) \Longrightarrow q^\beta \mid 2u \Longrightarrow \beta=0 \Longrightarrow r=u+q^\beta=2^m+1$。

$\therefore$ $q^{2n}=v^2=(r+u)(r-u)=2^{m+1}+1 \Longrightarrow (q^n+1)(q^n-1)=2^{m+1}$。

设 $q^n+1=2^l$，$q^n-1=2^t(l>t) \Longrightarrow q^n=\frac{1}{2}(2^l+2^t)=2^{l-1}+2^{t-1} \xrightarrow{q\text{ 是奇数}} t-1=0 \Longrightarrow t=1 \Longrightarrow q^n-1=2 \Longrightarrow q^n=3 \Longrightarrow q=3$，$n=1 \Longrightarrow v=q^n=3 \Longrightarrow q^n+1=4 \Longrightarrow 2^{m+1}=(q^n+1)(q^n-1)=4\times2=2^3 \Longrightarrow m=2 \Longrightarrow u=2^m=4$，$r=2^m+1=5$。

$\therefore$ $|AM|=1$，$|BM|=9$，$|CN|=8$，$|DN|=2$。

(ii) 设 v 为偶数，同理可得 $v=4$，$u=3$，这与 $u>v$ 的假设不符，故不可能。

第三章

1．若整数 $a=a_na_{n-1}\cdots a_2a_1a_0$（$a_n\neq0$，$0\leqslant a_i\leqslant9$，$i=0,1,$

…，n）。因为$1000\equiv1\pmod{37}$，令

$$f(a)=a_2a_1a_0+a_n\cdots a_5a_4a_3,$$

则$37|a\Longleftrightarrow37|f(a)$。从而得到 a 是否37的倍数的判别法。例如，若 $a=1249083$，由于

$$1249083\longrightarrow1332\longrightarrow333,\ 37|333,$$

则 $37|1249083$。

因为$100\equiv-1\pmod{101}$，令

$$f(a)=a_n\cdots a_4a_3a_2-a_1a_0,$$

则 $101|a\Longleftrightarrow101|f(a)$。从而得到 a是否101的倍数的一种判别法。例如，$a=3813659$，由于

$$3813659\longrightarrow38077\longrightarrow303,\ 101|303,$$

$\therefore$ $101|3813659$。

2.（i） 因为$4568\equiv4+5+6+8\equiv5\pmod 9$，$7391\equiv7+3+9+1\equiv2\pmod 9$，所以$4568\times7391\equiv5\times2\equiv1\pmod 9$，而 $30746529\equiv0\pmod 9$故计算是错误的。

（ii） $16\times937\times1559\equiv7\times1\times2\equiv5\pmod 9$，而$23373528\equiv6\pmod 9$，故计算是错误的。

3. 经检验知3、5是它的因子，故

```
3|1 5 3 5 6 2 5
   3|5 1 1 8 7 5
    3|1 7 0 6 2 5
      5|5 6 8 7 5
       5|1 1 3 7 5
         5|2 2 7 5
           5|4 5 5
             7|9 1
               1 3
```

$\therefore\ 1535625=3^3\times5^4\times7\times13$。

4. 是。因为$0\equiv0$，$2^1\equiv2$，$2^2=4$，$2^3\equiv8$，$2^4\equiv5$，$2^5\equiv10$，$2^6\equiv9$，$2^7\equiv7$，$2^8\equiv3$，$2^9\equiv6$，$2^{10}\equiv1\pmod{11}$是 0，1，…，10的一个排列。

5. 令$a=2m+1$，A，当$n=1$时，则$a^2=(2m+1)^2=4m(m+1)$

$+1\equiv 1 \pmod 8$)，故 $n=1$时结论成立。

B) 设 $n=k$时结论成立，即

$(2m+1)^{2^k}-1\equiv 0 \pmod{2^{k+2}} \Longrightarrow (2m+1)^{2^k}-1=2^{k+2}t$，$t$是整数。而

$a^{2^{k+1}}-1=(a^{2^k}-1)(a^{2^k}+1)=(a^{2^k}-1)[(a^{2^k}-1)+2]$

$=(t\cdot 2^{k+2})^2+2\cdot t\cdot 2^{k+2}=t^2 2^{2k+4}+t\ 2^{k+3}$

$=t2^{k+3}(t2^{k+1}+1)\equiv 0 \pmod{2^{k+3}}$。

故对于 $n\geqslant 1$时，结论成立。

6。对 u、v 的不同取值 x 共有$p^{s-t}\cdot p^t=p^s$个值。今证明这样的p^s个值，关于模 p^s是两两互不同余的。若

$u_1+p^{s-t}v_1\equiv u_2+p^{s-t}v_2 \pmod{p^s} \Longrightarrow u_1-u_2\equiv p^{s-t}(v_2-v_1)$ $\pmod{p^s} \Longrightarrow p^{s-t}|u_1-u_2$，即 $u_1\equiv u_2 \pmod{p^{s-t}} \Longrightarrow u_1=u_2$ $\Longrightarrow p^{s-t}v_1\equiv p^{s-t}v_2 \pmod{p^s} \Longrightarrow v_1\equiv v_2 \pmod{p^t}$即 $v_1=v_2$。

7。由定理3·5系 1 知道当 $n=2$时，结论成立。

B，设为$k-1$时，结论成立。即，若m_1，m_2，…，m_{k-1}两两互素时，$S'=M_1'x_1+M_2'x_2+\cdots+M_{k-1}'x_{k-1}$，当$x_1$，$x_2$，…，$x_{k-1}$分别过模$m_1$，$m_2$，…，$m_{k-1}$的完全剩余系时，$S'$过模 $m'=m_1m_2\cdots m_{k-1}$的完全剩余系。其中$m_iM_i'=m'(i=1,\ \cdots,\ k-1)$。

则增加m_k，使$(m_i,\ m_k)=1(i=1,\ \cdots,\ k-1)$，令$M_i=m_kM_i'$ $(i=1,\ \cdots,\ k-1)$，$m'=M_k=m_1\cdots m_{k-1}$，$m=m_kM_k=m_1m_2\cdots m_k$。因为$(m_k,\ m_i)=1(i=1,\ 2,\ \cdots,\ k-1) \Longrightarrow (m_k,\ M_k)=1$。令

$$x=M_kx_k+m_kS',$$

当x_k过模m_k的完全剩系，S'过模M_k的完全剩余系时，由定理 3·5 系 1知，x过模$m=m_kM_k=m_1m_2\cdots m_k$的完全剩余系。这就证明了所要的结论。

8。(i) 证明：当 $x_i=-1,\ 0,\ 1(i=0,\ 1,\ \cdots,\ n)$时，(a)过模 $2H+1=3^{n+1}$的绝对最小完全剩余系。也就是(a)表示$[-H,\ H]$

中的2H+1个整数。事实上，当 $x_i=-1, 0, 1$时，(a) 共有 3^{n+1} 个值。且两两互不相等。否则

$$3^n x_n' + 3^{n-1}x_{n-1}' + \cdots + 3x_1' + x_0' = 3^n x_n + 3^{n-1}x_{n-1} + \cdots + 3x_1$$

$$+ x_0 \Longrightarrow 3^n(x_n' - x_n) + 3^{n-1}(x_{n-1}' - x_{n-1}) + \cdots + 3(x_1' - x_1) =$$

$$= x_0 - x_0' \Longrightarrow 3 | x_0 - x_0' \Longrightarrow x_0 = x_0',\ \text{即} 3^{n-1}(x_n' - x_n) + \cdots +$$

$$+ x_1' - x_1 = 0 \Longrightarrow 3 | x_1' - x_1 \Longrightarrow x_1' = x_1 \Longrightarrow \cdots \Longrightarrow x_n' = x_n.$$

又(a)的最大值是

$$3^n + 3^{n-1} + \cdots + 3 + 1 = \frac{3^{n+1}-1}{3-1} = H;$$

(a)的最小值是

$$-3^n - 3^{n-1} - \cdots - 3 - 1 = -H,$$

故结论成立。

(ii) 特制 n+1个砝码分别重 1，3，3^2，…，3^n斤。把要称的物体及 x_i 取 -1的砝码放在天秤的右盘，x_i 取 1 的砝码放在左盘。

从(i)的结论，知道当 x_i 取适当的值时，可使$T = 3^n x_n + \cdots + 3x_1 + x_0$之值等于您所要称的物体的斤数（$\leqslant H$）。

(i)的另一种证法：整数 $-H, \cdots, -1, 0, 1, \cdots, H$ ($H = \frac{3^{n+1}-1}{3-1}$)是模$2H+1=3^{n+1}$的绝对最小完全剩余系。若用模2H+1的非负最小完全剩余系

$$0,\ 1,\ \cdots,\ H,\ H+1,\ \cdots,\ 2H$$

来代替，则当 $x_i' = 0, 1, 2$（$i = 0, 1, \cdots, n$）时

$$3^n x_n' + 3^{n-1}x_{n-1}' + \cdots + 3x_1' + x_0' \qquad (a)'$$

是一个三进位数，它共有 $3^{n+1}=2H+1$个不同的非负整数，其中最大的是

$$2(3^n + 3^{n-1} + \cdots + 3 + 1) = 2 \times \frac{3^{n+1}-1}{2} = 3^{n+1} - 1 = 2H.$$

所以(a)过模2H+1的非负完全剩余系。今考察：

$$3^n x_n' + 3^{n-1}x_{n-1}' + \cdots + 3x_1' + x_0' - H$$

$\because H = 3^n + 3^{n-1} + \cdots + 3 + 1$

$\therefore 3^n x_n' + 3^{n-1}x_{n-1}' + \cdots + 3x_1' + x_0' - H$

$$= 3^n(x_n' - 1) + 3^{n-1}(x_{n-1}' - 1) + \cdots + 3(x_1' - 1) + (x_0' - 1)$$

令 $x_i = x_i' - 1$，$(i = 0, 1, \cdots, n)$ 则得

$$3^n x_n + 3^{n-1}x_{n-1} + \cdots + 3x_1 + x_0 \quad \text{(a)}$$

从而知当 $x_i = -1, 0, 1$ 时(a)过模2H+1的绝对最小完全剩余系。故结论成立。

9．A）当 $k=2$ 时，x_1，x_2 分别过模 m_1，m_2 的完全剩余系时，$x_1 + m_1x_2$ 共有 m_1m_2 个值。且若

$$x_1 + m_1x_2 \equiv x_1' + m_1x_2' \pmod{m_1m_2} \Longrightarrow m_1(x_2 - x_2')$$

$$\equiv x_1' - x_1 \pmod{m_1m_2} \Longrightarrow m_1 | x_1' - x_1 \text{ 且 } x_2 - x_2'$$

$$\equiv \frac{x_1' - x_1}{m_1} \pmod{m_2} \Longrightarrow x_1 = x_1',\ x_2 = x_2'.$$

B）设当 $x_2, \cdots, x_k$ 分别过模 $m_2, \cdots, m_k$ 的完全剩余系时，$x_2 + m_2x_3 + \cdots + m_2\cdots m_{k-1}x_k$ 过模 $m_2\cdots m_k$ 的完全剩余系。因为 $(m_1, m_2\cdots m_k) = 1$，由定理3·5得，$m_1(x_2 + m_2x_3 + \cdots + m_2\cdots m_{k-1}x_k)$ 亦过模 $m_2\cdots m_k$ 的完全剩余系。

当 $x_1, x_2, \cdots, x_{k-1}, x_k$ 分别过模 $m_1, m_2, \cdots, m_{k-1}, m_k$ 的完全剩余系时，(a)有 $m_1m_2\cdots m_{k-1}m_k$ 个值，且由归纳法假设：

$$x_1 + m_1x_2 + \cdots + m_1\cdots m_{k-2}x_{k-1} + m_1\cdots m_{k-1}x_k$$

$$\equiv x_1' + m_1x_2' + \cdots + m_1\cdots m_{k-2}x_{k-1}' + m_1\cdots m_{k-1}x_k' \pmod{m_1\cdots m_k} \Longrightarrow x_1 \equiv x_1' \pmod{m_1},\ x_2 + m_2x_3 + \cdots + m_2\cdots m_{k-1}x_k \equiv$$

$\equiv x_2' + m_2x_3' + \cdots + m_2\cdots m_{k-1}x_k' \pmod{m_2\cdots m_k} \Longrightarrow$

$\Longrightarrow x_1 \equiv x_1' \pmod{m_1}$ $x_2 \equiv x_2' \pmod{m_2}$，…，$x_k \equiv x_k' \pmod{m_k}$

$\Longrightarrow x_1 = x_1'$，$x_2 = x_2'$，…，$x_k = x_k'$。

10。由定理3·5系2知，$a\xi$ 是过模m的互素剩余系a_1，a_2，…，$a_{\varphi(m)}$的，$0<a_i<m$，且$(a_i, m)=1$，$\left\{\frac{a_i}{m}\right\}=\frac{a_i}{m}(i=1, 2, \cdots, \varphi(m))$。

若$(a_i, m)=1$，$m>2$，则$(m-a_i, m)=1$，且$m-a_i \neq a_i$（否则$m=2a_i$，与$(a_i, m)=1$矛盾）。而$\frac{a_i+m-a_i}{m}=1$，$\varphi(m)$是偶数，且

$$\sum_\xi\left\{\frac{a\xi}{m}\right\}=\left\{\frac{a_1}{m}\right\}+\left\{\frac{a_2}{m}\right\}+\cdots+\left\{\frac{a_{\varphi(m)}}{m}\right\}$$

右边每一项$\left\{\frac{a_i}{m}\right\}$都存在另一项$\left\{\frac{m-a_i}{m}\right\}=\left\{\frac{a_j}{m}\right\}(i \neq j)$，使得$\left\{\frac{a_i}{m}\right\}+\left\{\frac{a_j}{m}\right\}=\frac{a_i}{m}+\frac{a_j}{m}=1$，右边共有$\frac{\varphi(m)}{2}$对，所以

$$\sum_\xi\left\{\frac{a\xi}{m}\right\}=\frac{1}{2}\varphi(m)。$$

当$m=2$时，$\varphi(2)=1$，$\sum_\xi\left\{\frac{a\xi}{m}\right\}=\frac{1}{2}$。

11。由定理3·5系3知道当$k=2$时，结论成立。

设$k-1$时，结论成立。即$m'=m_1\cdots m_{k-1}=m_iM_i'$（$i=1, \cdots, k-1$），$(m_i, m_j)=1(i\neq j=1, \cdots, k-1)$，$\xi_1$，$\xi_2$，…，$\xi_{k-1}$分别过模$m_1$，$m_2$，…，$m_{k-1}$时，

$$T_{k-1} = M_1'\xi_1+M_2'\xi_2+\cdots+M_{k-1}'\xi_{k-1} \qquad (2)$$

过模$m'=m_1m_2\cdots m_{k-1}$的互素剩余系，其中$M_i'm_i=m'(i=1, 2,$

$\cdots, k-1$）

（2）的两边同乘以m_k，$(m_k, m_i)=1$（$i=1, \cdots, k-1$），再加上$M_k\xi_k$（$M_k=m'$），得

$$T_k = M_1\xi_1 + M_2\xi_2 + \cdots + M_{k-1}\xi_{k-1} + M_k\xi_k$$
$$= m_k\eta + M_k\xi \quad (1)$$

其中η和ξ分别过模$M_k=m'$和m_k的互素剩余系，由定理3·5系3知道T_k过模$M_k\cdot m_k = m_1m_2\cdots m_k = m$的互素剩余系。

12. 因为$63=3^2\times 7$，$\varphi(63)=\varphi(3^2)\varphi(7)=36$，而$7222=2\times 23\times 157$，所以$(63, 7222)=1$，由欧拉定理，知

$(7222^{37}+3)^{18} \equiv (7222+3)^{18} \equiv (43)^{18} \equiv (-20)^{18} \pmod{63}$ 而

$(-20)^2 \equiv 22$，$(-20)^3 \equiv 1$，$(-20)^{18} \equiv 1 \pmod{63}$

$\therefore \quad (7222^{37}+3)^{18} \equiv 1 \pmod{36}$。

13. (i) A）当$t=2$时，按二项式展开得

$$(h_1+h_2)^p \equiv h_1^p + h_2^p \pmod p。$$

B） 设$t=k$时，结论成立。即

$$(h_1+h_2+\cdots+h_k)^p \equiv h_1^p + h_2^p + \cdots + h_k^p \pmod p。$$

当$t=k+1$时，

$$(h_1+h_2+\cdots+h_k+h_{k+1})^p \equiv (h_1+\cdots+h_k)^p + h_{k+1}^p$$
$$\equiv h_1^p + \cdots + h_k^p + h_{k+1}^p \pmod p。$$

(ii) 取$h_1=h_2=\cdots=h_t=1$（$t=1, 2, \cdots$），得

$$t^p \equiv t \pmod p。$$

(iii) 设$m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$，$\varphi(m)=\prod_{i=1}^{s}(p_i-1)p_i^{\alpha_i-1}$，因为对于任一素数p，若$(a, p)=1$，则$a^{p-1}\equiv 1 \pmod p$，即存在k使得$a^{p-1}=1+kp$。而

$$(a^{p-1})^p = (1+kp)^p = 1 + c_p^1 kp + \cdots + (kp)^p = 1+p^2 l$$

$\equiv 1 (\bmod p^2)$.

依此类推可得 $a^{(p-1)p^{\alpha-1}} \equiv 1 (\bmod p^{\alpha})$ 即 $a^{\varphi(p^{\alpha})} \equiv 1 (\bmod p^{\alpha})$.

若 $(a, m) = 1$，则 $(a, p_i^{\alpha_i}) = 1$ $(i = 1, 2, \cdots, s)$，因而

$$a^{\varphi(p_i^{\alpha_i})} \equiv 1 (\bmod p_i^{\alpha_i}) \xrightarrow{3^\circ} a^{\varphi(m)} \equiv 1 (\bmod p_i^{\alpha_i}) (i = 1, \cdots, s) \xrightarrow{11^\circ} a^{\varphi(m)} \equiv 1 (\bmod [p_1^{\alpha_1}, p_2^{\alpha_2}, \cdots, p_s^{\alpha_s}])$$

$\therefore$ $a^{\varphi(m)} \equiv 1 (\bmod m)$.

第四章

1. (i) $337 : 256 = 1$

$256 : 81 = 3$

$81 : 13 = 6$

$13 : 3 = 4$

$3 : 1 = 3$

$\therefore$ $\frac{337}{256} = [1, 3, 6, 4, 3]$, $\frac{}{1}\frac{4}{4}\frac{6}{25}\frac{3}{79}\frac{1}{104}$.

256×104的末位数字是4，337×79的末位是3，故

$256 \times 104 \equiv 1 (\bmod 337) \Longrightarrow x = 104 \times 176 \equiv 81$. $(\bmod 337)$

(ii) 因 $(258, 348) = 6$，$6 \nmid 131$，故无解.

(iii) $\because 3 \times 10 \equiv 1 (\bmod 29)$，且 $(10, 29) = 1$，

$\therefore$ $10 \times 3x \equiv 10 \times 10 \equiv 13 (\bmod 29) \Longrightarrow x \equiv 13 (\bmod 29)$

(iv) $\because$ $\frac{111}{47} = [2, 2, 1, 3, 4]$.

$\frac{}{1}\frac{3}{3}\frac{1}{4}\frac{2}{11}\frac{2}{26}$.

47×26的末位数字是2，111×11的末位是1，所以

$47 \times 26 \equiv 1 (\bmod 111) \Longrightarrow x \equiv 26 \times 89 \equiv -17 (\bmod 111)$

(v) 因为 $(660, 1385) = 5$，$5 | 595$，所以原同余式及模除以5得

$132x \equiv 119 \pmod{277}$

$\because \quad \frac{277}{132} = [2, 10, 6, 2]$, $\quad \frac{}{1} \quad \frac{6}{6} \quad \frac{10}{61} \quad \frac{2}{128}$

132×128的末位是 6，61×277的末位是 7，所以

$132 \times (-128) \equiv 1 \pmod{277} \Longrightarrow x \equiv -128 \times 119$

$\equiv 3 \pmod{277}$。

$\therefore \quad x \equiv 3,\ 280,\ 557,\ 834,\ 1111 \pmod{1385}$

是原同余式的五个解。

（vi） 因为$(1215, 2755) = 5$，故先解

$243x \equiv 112 \pmod{551}$，

同上小题的方法，解得

$x \equiv 200,\ 751,\ 1302,\ 1853,\ 2404 \pmod{2755}$，

是原同余式的解。

2 由定理 4·1 知该同余式有解，若$(2^k, b) = 2^s$，则由同余的性质7°知它与$2^{k-s}x \equiv \frac{b}{2^s} \pmod{m}$等价，故可设$(2^k, b) = 1$。因为 b 和 m 都是奇数，所以 $b+m$ 和 $b-m$中总有一数是 4 的倍数，记作$b \pm m \equiv 0 \pmod 4$，事实上，$b = 2t+1$，$m = 2u+1$则$b+m = 2(t+u-1)$；$b-m = 2(t-u)$。当 t、u 一奇一偶时 $4|b+m$；当 t，u 同奇或同偶时，$4|b-m$。

设 $2^\delta \| b \pm m$（"$\|$"表示$2^\delta | b \pm m$，$2^{\delta+1} \nmid b \pm m$）。

于是

（i） 若$\delta \geqslant k$，则 $x \equiv \frac{b \pm m}{2^k} \pmod{m}$是该同余式的解。

（ii） 若$\delta < k$，令$b_1 = \frac{b \pm m}{2^\delta}$，则它与

$$2^{k-\delta}x \equiv b_1 \pmod{m}$$

等价。继续这种方法，容易求出该同余式的解。

3. $2^6 x \equiv 179 \pmod{337}$ （a）

因为 $b+m=179+337=4\times129$，所以（a）与

$$2^6x\equiv129\ (\mathrm{mod}\ 337)\qquad (a')$$

等价。又因 $129-337=-2^4\times13$，所以（a′）与

$$2^2x\equiv-13\ (\mathrm{mod}\ 337)\qquad (a'')$$

等价，而 $-13+337=2^2\times81$，所以

$$x\equiv81\ (\mathrm{mod}\ 337)$$

是（a）的解。

4. 与第2题一样地，可设 $(b,3)=1$，因此

$$b=\begin{cases}3t+1\begin{cases}m=3t'+1\Longrightarrow 3\mid b-m;\\ m=3t'+2\Longrightarrow 3\mid b+m;\end{cases}\\ 3t+2\begin{cases}m=3t'+1\Longrightarrow 3\mid b+m;\\ m=3t'+2\Longrightarrow 3\mid b-m.\end{cases}\end{cases}$$

所以3整除 $b+m$ 或 $b-m$ 之一，若 $3^\delta \| b\pm m$，则（a）等价于

$$3^{k-\delta}\equiv\frac{b\pm m}{3^\delta}\ (\mathrm{mod}\ m).\qquad (a')$$

依此类推可得与第二题类似的一种解法。

5. 先解

$$3^5x\equiv112\ (\mathrm{mod}\ 551).\qquad (a)$$

因为 $112+551=3\times221$，所以（a）等价于

$$3^4x\equiv221\ (\mathrm{mod}\ 551);\qquad (a')$$

又因 $221-551=3\times(-110)$，所以（a′）等价于

$$3^3x\equiv-110\ (\mathrm{mod}\ 551);\qquad (a'')$$

又因 $-110+551=3^2\times49$，所以（a″）等价于

$$3x\equiv49\ (\mathrm{mod}\ 551).\qquad (a''')$$

（a‴）有解 $x\equiv200\ (\mathrm{mod}\ 551)$，所以原同余式有解

$$x\equiv200,\ 751,\ 1302,\ 1853,\ 2404\ (\mathrm{mod}\ 2755)$$

6. 设 $a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$，若 $b+mt\equiv0\ (\mathrm{mod}\ p_1)$ 且 $p_1^{\delta_1}\| b+mt$，则（1）等价于

$$p_1^{\alpha_1-\delta_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} x \equiv \frac{b+mt}{p_1^{\delta_1}} \pmod{m}. \tag{2}$$

今用数学归纳法证明之。

A）当 $k=1$时，（1）等价于

$$p_1^{\alpha_1-\delta_1} x \equiv b_1 \pmod{m}, \quad b_1=\frac{b+mt}{p_1^{\delta_1}},$$

依此类推，可得 $x\equiv c \pmod{m}$ 是（1）的解。

B）设 $k-1$ 时结论成立，即

$$p_1^{\alpha_1} \cdots p_{k-1}^{\alpha_{k-1}} x \equiv b \pmod{m},$$

可用上法求得 $x\equiv c \pmod{m}$ 是它的解。而

$$p_1^{\alpha_1} \cdots p_{k-1}^{\alpha_{k-1}} p_k^{\alpha_k} x \equiv b \pmod{m} \Longrightarrow p_1^{\alpha_1} \cdots p_{k-1}^{\alpha_{k-1}} y \equiv b \pmod{m},$$

其中$y=p_k^{2k} x \xrightarrow{\text{归纳假设}} y\equiv c \pmod{m}$，即$p_k^{2k} x\equiv c, \pmod{m}$

$\xrightarrow{\text{由A，}} x\equiv c' \pmod{m}$是（1）的解。

例，因为$1269=2^4 3^4$，$1935=3^2\times 5\times 43=3^2\times 215$，$1125=3^2\times 125$，故先解

$$2^4 3^2 x\equiv 125 \pmod{215}.$$

由于 $2^2 \| 125+215$，

$\therefore$ $2^2\cdot 3^2 x\equiv \frac{125+215}{4}\equiv 85 \pmod{215} \Longrightarrow 2^2\cdot 3^2 x$

$\equiv 300 \pmod{215} \Longrightarrow 3^2 x\equiv 75 \pmod{215} \Longrightarrow 3x\equiv 25 \pmod{215}$

$\Longrightarrow 3x\equiv 25+215=240 \pmod{215} \Longrightarrow x\equiv 80 \pmod{215}$.

$\therefore$ $x\equiv 80+215t \pmod{1935}$，$t=0, 1, \cdots, 8$

是该同余式的 9 个解。

注：习题2，4，6给我们一种较简单的解一元一次同余式的方法。

7. $\begin{cases} x+4y\equiv 29 \pmod{143}, \\ 2x-9y\equiv 59 \pmod{143}; \end{cases} \Longrightarrow \begin{cases} x+4y\equiv 29 \pmod{143}, \\ 17y\equiv -1 \pmod{143}; \end{cases}$

$$\Longrightarrow \begin{cases} x+4y\equiv 29 \pmod{143}, \\ y\equiv 42 \pmod{143}; \end{cases} \Longrightarrow \begin{cases} x\equiv 4, \\ y\equiv 42. \end{cases} \pmod{143}.$$

8．即解

$2x\equiv 1 \pmod 7 \Longrightarrow x\equiv 4 \pmod 7$，即 $\frac{1}{2}\equiv 4 \pmod 7$

$3x\equiv 1 \pmod 7 \Longrightarrow x\equiv 5 \pmod 7$，即 $\frac{1}{3}\equiv 5 \pmod 7$

同理易得 $\frac{1}{4}\equiv 2$，$\frac{1}{5}\equiv 3$，$\frac{1}{6}\equiv 6 \pmod 7$。

9．即解下之同余式

$47x\equiv 1 \pmod{93} \Longrightarrow x\equiv 2 \pmod{93}$，即 $\frac{1}{47}\equiv 2 \pmod{93}$。

同样地，可得 $\frac{23}{37}\equiv 29 \pmod{50}$，$\frac{49}{102}\equiv 42 \pmod{12}$。

10．（i） 当 $(a, m)=(k, m)=1$ 时，$ax\equiv b \pmod m$ 等价于 $akx\equiv bk \pmod m \Longrightarrow \frac{b}{a}\equiv\frac{bk}{ak} \pmod m$。

（ii） $\because a_1x_1\equiv b_1$，$a_2x_2\equiv b_2 \pmod m$，$(a_1, m)=(a_2, m)=1$

$\Longrightarrow a_1a_2x_1\equiv a_2b_1$，$a_1a_2x_2\equiv a_1b_2 \pmod m$

$\Longrightarrow a_1a_2(x_1\pm x_2)\equiv a_2b_1\pm a_1b_2$ 且 $x_1\equiv\frac{b_1}{a_1}$

$x_2\equiv\frac{b_2}{a_2} \pmod m$

$\Longrightarrow \frac{b_1}{a_1}\pm\frac{b_2}{a_2}\equiv\frac{a_2b_1\pm a_1b_2}{a_1a_2} \pmod m$。

（iii） 因 $a_1x_1\equiv b_1$，$a_2x_2\equiv b_2 \pmod m$，$(a_1, m)=(a_2, m)=1$

$\Longrightarrow a_1a_2x_1x_2\equiv b_1b_2 \pmod m$ 且 $(a_1a_2, m)=1$

$\Longrightarrow \frac{b_1}{a_1}\cdot\frac{b_2}{a_2}\equiv\frac{b_1b_2}{a_1a_2} \pmod m$。

（iv） $a_1x_1\equiv b_1$，$a_2x_2\equiv b_2$，$b_2x_2'\equiv a_2 \pmod m$

$\Longrightarrow a_1b_2x_1x_2'\equiv b_1a_2$，$a_2b_2x_2x_2'\equiv a_2b_2 \pmod m$，

且因 $(a_1, m)=(a_2, m)=(b_2, m)=1 \Longrightarrow x_1x_2' \equiv \frac{b_1a_2}{a_1b_2}$，

$x_2x_2' \equiv 1 \pmod m$ 且 $(x_2, m)=(x_2', m)=1$。

又 $\frac{b_2}{a_2}x \equiv \frac{b_1}{a_1} \pmod m \Longrightarrow x_2x \equiv x_1$，因 $(x_2, m)=1$，

$x_2x_2' \equiv 1 \pmod m \Longrightarrow x \equiv x_1x_2' \pmod m \Longrightarrow \frac{x_1}{x_2}$

$\equiv x_1x_2' \pmod m$。

$\therefore \frac{b_1}{a_1} : \frac{b_2}{a_2} \equiv \frac{b_1a_2}{a_1b_2} \pmod m$．

11. 若 $(a, m)=1$ 由例3·7知道，$ax \equiv b \pmod m$ 的解数

$$T=\frac{1}{m}\sum_{x=0}^{m-1}\sum_{k=0}^{m-1} e^{\frac{1}{m}2\pi ik(ax+b)}$$

因为 $(a, m)=1$，$x=0, 1, 2, \cdots, m-1$ 时 $ax-b$ 过模 m 的完全剩余系，故其中必有一个且只有一个 x 的值使 $ax-b\equiv 0 \pmod m$，所以 $T=1$，即 $ax\equiv b \pmod m$ 有唯一解。

若 $(a, m)=d>1$．

（i） 若 $d \nmid b$ 时，则 $d \nmid ax-b \Longrightarrow m \nmid ax-b \Longrightarrow T=0$，即 $ax\equiv b \pmod m$ 无解。

（ii） 若 $d|b$ 时，令 $a_1d=a$，$b_1d=b$，$m_1d=m$，则

$$T=\frac{1}{m}\sum_{x=0}^{m-1}\sum_{k=0}^{m-1} e^{2\pi ik\left(\frac{ax-b}{m}\right)}=\frac{1}{m}\sum_{x=0}^{m-1}\sum_{k=0}^{m-1} e^{2\pi ik(a_1x-b_1}$$，

当 $x=0, 1, \cdots, m-1$ 时，$T=1$，所以当 $x=0, 1, \cdots, m-1$ 时，$T=\frac{m}{m_1}=d$，即原同余式有 d 个解。

12. 用孙子定理求解

（i） $x\equiv 3\times 22+5\times 56\equiv 38 \pmod{77}$。

（ii） $M=11\times 7\times 5=385$，$M_1'M_1=210$，$M_2'M_2=330$，$M_3'M_3=231$，

$\therefore$ $x\equiv 2\times 210+5\times 330+4\times 231\equiv 299 \pmod{385}$。

(iii) 原同余式等价于

$$\begin{cases} x\equiv 1 \pmod 7, \\ x\equiv 3 \pmod 5, \\ x\equiv 5 \pmod 9. \end{cases}$$

而$M=315$，$M_1'M_1=225$，$M_2'M_2=126$，$M_3'M_3=280$或$M_3'M_3=-35$。

$\therefore\quad x\equiv 225+3\times 126-5\times 35\equiv 113 \pmod{315}$。

13. (i) 即解

$$\begin{cases} x\equiv 1 \pmod 7 \\ x\equiv 2 \pmod 8 \\ x\equiv 4 \pmod 9 \end{cases} \Longrightarrow x\equiv 1\times 288+2\times 441+4\times 280\equiv 274 \pmod{504}$$

(ii) $$\begin{cases} x\equiv 1 \pmod 2 \\ x\equiv 2 \pmod 5 \\ x\equiv 3 \pmod 7 \\ x\equiv 5 \pmod 9 \end{cases} \Longrightarrow x\equiv 1\times 315+2\times 126+3\times 540+5\times 280\equiv 437 \pmod{630}.$$

(iii) $$\begin{cases} x\equiv 3 \pmod{11} \\ x\equiv 2 \pmod{72} \\ x\equiv 1 \pmod{13} \end{cases} \Longrightarrow 3\times 936+2\times(-143)+1\times(-792)\equiv 1730 \pmod{10296}.$$

14. $\because$ $[m_1, m_2] \mid x-a \Longrightarrow m_1 \mid x-a$, $m_2 \mid x-a \Longrightarrow x\equiv a \pmod{m_1}$, $x\equiv a \pmod{m_2}$，所以(β)是(α)的解

如果α还有一个解$x\equiv a_1 \pmod{m_1}$ $x\equiv a_1 \pmod{m_2}$，那么$m_1 \mid x-a_1$, $m_2 \mid x-a_1 \Longrightarrow [m_1, m_2] \mid x-a_1$ $\Longrightarrow x\equiv a_1 \pmod{[m_1, m_2]} \Longrightarrow a_1\equiv a \pmod{[m_1, m_2]}$，所以(α)只有形如(β)的唯一解。

实际上，此题亦可由定理4·6及4·4直接推得。

15. 如果(a)有解$x\equiv\alpha \pmod{[m_1, \cdots, m_k]}$，那末

$m_i|\alpha-b_i$（$i=1$，2，…，k），又$n_i|m_i\Longrightarrow n_i|\alpha-b_i$（$i=1$，2，…，$k$）$\Longrightarrow\alpha\equiv b_i\pmod{n_i}$（$i=1$，2，…，$k$）。

又因$(n_i, n_j)=1$（$i\neq j=1$，2，…，k），由孙子定理知（b）只有唯一解，（a）亦只有唯一解且（a）的解也是（b）的解，故（a）与（b）同解。

16.（i） $m_1=7$，$m_2=9=3\times3$，$m_3=15=3\times5$，$[m_1, m_2, m_3]=315$，取$n_1=7$，$n_2=9$，$n_3=5$，$[n_1, n_2, n_3]=315$，且$(n_1, n_2)=(n_2, n_3)=(n_1, n_3)=1$ 由15题知，只需解

$$\begin{cases} x\equiv2\pmod 7, \\ x\equiv5\pmod 9, \\ x\equiv1\pmod 5. \end{cases}$$

用孙子定理，仿12题（iii），解得$x\equiv86\pmod{315}$。

（ii） 用"$\cong$"表示二方程组等价，则按题意

$$\begin{cases} x\equiv0\pmod 5, \\ x\equiv10\pmod{715}, \\ x\equiv140\pmod{247}, \\ x\equiv245\pmod{391}, \\ x\equiv109\pmod{187}, \end{cases} \cong \begin{cases} x\equiv0\pmod 5, \\ x\equiv10\pmod{143}, \\ x\equiv7\pmod{19}, \\ x\equiv15\pmod{23}, \\ x\equiv7\pmod{17}. \end{cases}$$

解得 $x\equiv10020\pmod{5311735}$。

17. 设甲、乙两港的距离 x 公里，则

$$\begin{cases} x\equiv0\pmod{300}, \\ x\equiv18\times\frac{240}{24}\equiv180\pmod{240}, \\ x\equiv8\times\frac{180}{24}\equiv60\pmod{180}, \end{cases} \cong \begin{cases} x\equiv0\pmod{5^2}, \\ x\equiv4\pmod{2^4}, \\ x\equiv6\pmod{3^2}. \end{cases}$$

解得$x\equiv3300\pmod{3600}$，所以甲、乙两港距离3300公里，第一号船行$\frac{3300}{300}=11$（天），第二号船行$\frac{3300}{240}=13\frac{18}{24}$（天），第三号船行$\frac{3300}{180}=18\frac{8}{24}$（天）。

18. (i)

$$\begin{array}{l} 3+0+1+5-2 \mid \underline{1} \\ \quad\ \ 3+3+4+2 \\ \hline 3+3+4+2 \end{array}$$

∴ $3x^4+x^2+5x-2\equiv(x-1)(3x^3+3x^2+4x+2)\pmod 7$.

(ii) 经试验知其不可约

(iii)

$$\begin{array}{l} 1+0-2+1+4 \mid \underline{2} \\ \quad +2+4+4-4 \\ \hline 1+2+2-2 \mid \underline{3} \\ \quad +3-6+9 \\ \hline 1-2+3 \end{array}$$

∴ $x^4-2x^2+x+4\equiv(x-2)(x-3)(x^2-2x+3)\pmod 7$.

19. 与上题同一方法可得

(i) 原式$\equiv 2(x-2)(x-3)(x^2-2)\pmod{11}$；

(ii) 原式$\equiv(x-2)^2(x-3)(x-4)\pmod{11}$.

20 (i) ∵ $x^7-6\equiv(x^5-x)x^2+(x^3-6)\equiv x^3-1\pmod 5$

故它只有一个解 $x\equiv 1\pmod 5$.

(ii) 因为原同余式等价于$2x^3+3\equiv 0\pmod 5$，故它只有一个解 $x\equiv 1\pmod 5$

(iii) 原同余式等价于

$$\begin{cases} x^2-x\equiv 0\pmod 2, & (1)\\ 2x+2\equiv 0\pmod 3, & (2)\\ x^3+2x^2+2x\equiv 0\pmod 5. & (3)\end{cases}$$

(1) 有解 $x\equiv 0,\ 1\pmod 2$；

(2) 有解 $x\equiv 2\pmod 3$；

(3) 有解 $x\equiv 0,\ 1,\ 2\pmod 5$.

∴ $\begin{cases} x\equiv 0\pmod 2,\\ x\equiv 2\pmod 3,\\ x\equiv 0\pmod 5;\end{cases}$ $\begin{cases} x\equiv 0\pmod 2,\\ x\equiv 2\pmod 3,\\ x\equiv 1\pmod 5;\end{cases}$ $\begin{cases} x\equiv 0\pmod 2,\\ x\equiv 2\pmod 3,\\ x\equiv 2\pmod 5.\end{cases}$

$$\begin{cases} x\equiv 1 \pmod 2, \\ x\equiv 2 \pmod 3, \\ x\equiv 0 \pmod 5; \end{cases} \quad \begin{cases} x\equiv 1 \pmod 2, \\ x\equiv 2 \pmod 3, \\ x\equiv 1 \pmod 5; \end{cases} \quad \begin{cases} x\equiv 1 \pmod 2, \\ x\equiv 2 \pmod 3, \\ x\equiv 2 \pmod 5. \end{cases}$$

用孙子定理，$x\equiv b_1\times 15+b_2\times 10+b_3\times 6 \pmod{30}$，故其解为

$x_1\equiv 20$，$x_2\equiv 26$，$x_3\equiv 2$，$x_4\equiv 5$，$x_5\equiv 11$，$x_6\equiv 17 \pmod{30}$。

(iv) 因$225=3^2\times 5^2$，故原同余式等价于

$$\begin{cases} 4x^4+3x^3+6x+2\equiv 0 \pmod{3^2}, \\ 6x^4+7x^3-4x-9\equiv 0 \pmod{5^2}. \end{cases}$$

先解，$4x^4+3x^3+6x+2\equiv 0 \pmod 3 \Longrightarrow x^4-1\equiv 0 \pmod 3$ $\cong x^2-1\equiv 0 \pmod 3$（$\because x^4-1\equiv (x^3-x)x+(x^2-1) \pmod 3$）。

故有二解 $x\equiv \pm 1 \pmod 3$。而

$f'(x)=16x^3+9x^2+6 \Longrightarrow f'(1)=31$，$3\nmid 31$，$f'(-1)=-7$，$3\nmid(-7)$。

$$t_1 f'(1)\equiv -\frac{f(1)}{3}=-5\equiv 1 \pmod 3 \Longrightarrow t_1'\equiv 1 \pmod 3),$$

故 $x_1\equiv 1+3(1+3t_2)=4+9t_2$（$t_2=0, \pm 1, \pm 2, \cdots$）。

同理 $x_2\equiv 5 \pmod 9$，故第一式有两个解 $x_1\equiv 4$，$x_2\equiv 5 \pmod 9$。

又 $g(x)=6x^4+7x^3-4x-9\equiv x^4+2x^3+x+1\equiv 0 \pmod 5$ 有且只有二解 $x\equiv 1, 2 \pmod 5$，且 $g(1)=0$，$g(2)=135$，$g'(x)=24x^3+21x^2-4$，$g'(1)=41$，$5\nmid 41$；$g'(2)=272$，$5\nmid 272$，所以

$$41t_1\equiv 0 \pmod 5 \Longrightarrow t_1=0 \Longrightarrow x_1'\equiv 1 \pmod{25}.$$

$$272t_1\equiv -27 \pmod 5 \Longrightarrow t_1=4 \Longrightarrow x_2'\equiv 2+5\times 4$$

$$\equiv -3 \pmod{25}.$$

故第二式有且只有 $x\equiv 1, -3 \pmod{25}$ 二解。

$$\therefore \begin{cases} x\equiv 4 \pmod 9, \\ x\equiv 1 \pmod{25}; \end{cases} \quad \begin{cases} x\equiv 4 \pmod 9, \\ x\equiv -3 \pmod{25}; \end{cases} \quad \begin{cases} x\equiv 5 \pmod 9, \\ x\equiv 1 \pmod{25} \end{cases}$$

$$\begin{cases} x \equiv 5 \pmod{9}, \\ x \equiv -3 \pmod{25}. \end{cases}$$

由孙子定理 $x \equiv b_1 \times 100 + b_2 \times 126 \pmod{225}$，

所以原同余式，有且只有 $x \equiv 76$，22，176，122（mod225）四个解。

21.（i） 因为 $x^7 - x = (x^2 + 2x - 1)(x^5 - 2x^4 + 5x^3 - 12x^2 + 29x - 70) + 168x + 70$，而 $168x + 70 \equiv 0 \pmod{7}$，故它有两个不同的解。

（ii） 因为 $x^7 - x = (x^3 + x - 3)(x^4 - x^2 + 3x + 1) + 7x + 3$，而 $7x - 3 \equiv -3 \pmod{7}$ 故该同余式无三个不同的解。

22. 若 $(x_1^0, x_2^0, \cdots, x_n^0)$ 是（1）的一个解则

$$l_i(x_1^0, \cdots, x_n^0) \equiv 0 \pmod{m} \quad (i = 1, \cdots, k) \xrightarrow{(c_i,\ m) = 1}$$

$$c_1 l_1(x_1^0, \cdots, x_n^0) + \cdots + c_i l_i(x_1^0, \cdots, x_n^0) + \cdots + c_k l_k(x_1^0, \cdots, x_n^0) \equiv 0 \pmod{m}$$

反之，若 $(c_i, m) = 1$，且 $(x_1^0, \cdots, x_n^0)$ 是（2）的解，则对模 m 来说

$$\begin{cases} l_1(x_1^0, \cdots, x_n^0) \equiv 0, \\ \cdots \quad \cdots \quad \cdots \quad \cdots, \\ l_{i-1}(x_1^0, \cdots, x_n^0) \equiv 0, \\ c_1 l_1(x_1^0, \cdots, x_n^0) + \cdots + c_i l_i(x_1^0, \cdots, x_n^0) + \cdots + \\ \qquad\qquad c_k l_k(x_1^0, \cdots, x_n^0) \equiv 0, \\ l_{i+1}(x_1^0, \cdots, x_n^0) \equiv 0, \\ \cdots \quad \cdots \quad \cdots \quad \cdots, \\ l_k(x_1^0, \cdots, x_n^0) \equiv 0. \end{cases}$$

因而上之第 i 式是：

$$c_1\times 0+\cdots+c_i l_i(x_1^0,\cdots,x_n^0)+\cdots+c_k\times 0\equiv 0(\bmod m)$$

$$\Longrightarrow c_i l_i(x_1^0,\cdots,x_n^0)\equiv 0(\bmod m)$$

$$\xrightarrow{(c_i,\ m)=1} l_i(x_1^0,\cdots,x_n^0)\equiv 0(\bmod m),$$

所以$(x_1^0,\cdots,x_n^0)$亦(1)的解，即(1)≃(2)。

取 $c_1=\begin{vmatrix}-2 & 1\\ 2 & -3\end{vmatrix}\equiv 4(\bmod 9)$，$c_2=-\begin{vmatrix}1 & -1\\ 2 & -3\end{vmatrix}\equiv$

$\equiv 1(\bmod 9)$，$c_3=\begin{vmatrix}1 & -1\\ -2 & 1\end{vmatrix}\equiv -1(\bmod 9)$，则

$c_1l_1+c_2l_2+c_3l_3=(8x+4y-4z-20)+(3x-2y+z-4)$
$-(x+2y-3z-6)\equiv 10x\equiv 0(\bmod 9)\Longrightarrow x\equiv 0(\bmod 9)$。代入第一、二式得

$$\begin{cases}y-z\equiv 5\\ -2y+z\equiv 4\end{cases}(\bmod 9)\Longrightarrow\begin{cases}y\equiv 0\\ z\equiv 4\end{cases}(\bmod 9)$$

故其解是$(x,y,z)=(0,0,4)$。

23. 设x为红灯的盏数，则

$$\begin{cases}x\equiv 0(\bmod 5),\\ x\equiv 2(\bmod 7),\\ x\equiv 4(\bmod 9),\end{cases}\Longrightarrow x\equiv 310(\bmod 315)$$

24. 因为 v→22，i→9，c→3，t→20，0→15，r→18，所以有如下两种解答方法：

(i) 若解答矩阵的意义是：以密码所对应的数字(模29的一个类)，作为如下同余式组的解答

$$\begin{cases}2x+y-z\equiv b_1,\\ 3x-2y+z\equiv b_2,\ (\bmod 29)\\ x+2y-3z\equiv b_3,\end{cases}\qquad(\alpha)$$

求出b_1，b_2，b_3为其破译的密码。则以$(x,y,z)=(22,9,3)$

及（20，15，18）分别代入（2），得（b_1，b_2，b_3）=（21，22，2）及（8，19，25）（mod 29），故破译为u v b h s y。

（ii） 因为 $\begin{vmatrix} 2 & 1 & -1 \\ 3 & -2 & 1 \\ 1 & 2 & 3 \end{vmatrix} \equiv 10 \not\equiv 0 \pmod{29}$，

若以（22，9，3）及（20，15，18）分别代（α）的（b_1，b_2，b_3），依次解两组同余式，得（x，y，z）=（21，16，7）及（28，18，25），故破译为 u p g · r y。

25. 若（2）有解，令其解为 $x \equiv x_0 \pmod p$，$p-1=kn$，因为（a，p）=1，所以（x_0，p）=1．

$$x_0^{p-1} = x_0^{kn} \equiv 1 \pmod p，\ 又 x_0^n \equiv a \pmod p \Longrightarrow a^{\frac{p-1}{n}} \equiv 1 \pmod p.$$

反之，若$a^{\frac{p-1}{n}} \equiv 1 \pmod p$，则把(α)的两边用作$\frac{p-1}{n}$次乘方，得

$$x^{p-1} \equiv 1 \pmod p,$$

它有p－1个解，实际上"乘方"即在 $x^n - a \equiv 0 \pmod p$ 的左边乘上

$$g(x) = [\, x^{(p-1)-n} + a x^{(p-1)-2n} + \cdots + a^{\frac{p-1}{n}-2} x^n + a^{\frac{p-1}{n}-1} \,].$$

所以

$$x^{p-1} - 1 = (x^n - a) g(x) \equiv 0 \pmod p.$$

刚好有p－1个解，且因p是素数，故g(x)无多于(p－1)－n个解，即(α)刚好有n个解。

26. 当 $x \equiv x_0$，$x \equiv x_1 \pmod m$，是 $x^n \equiv a \pmod m$ 的解时，$x_1^n \equiv x_0^n \equiv a \pmod m$，因为（a，m）=1 故（$x_0$，m）=（$x_1$，m）=1，由定理3·5系2知道∃y∋ $y x_0 \equiv x_1 \pmod m$

$\Longrightarrow y^n x_0^n \equiv x_0^n \pmod m \Longrightarrow y^n \equiv 1 \pmod m$，

第五章

1. 由威尔逊（wilson）定理，

$(4m)!+1\equiv 0 \pmod{4m+1} \Longrightarrow 0\equiv(2m)!(4m)$
$(4m-1)\cdots(2m+1)+1\equiv(2m)!(4m+1-1)(4m+1-2)\cdots$
$(4m+1-2m)+1\equiv(2m)!(-1)^{2m}(2m)!+1\equiv[(2m)!]^2+1$
$\pmod{4m+1}$.

所以 $x\equiv\pm(2m)! \pmod p$ 是 $x^2+1\equiv 0 \pmod p$ 的两个解，且它再无其他的解了。

2. 因为 $72=2^3\times 3^2$，所以（a）与

$$\begin{cases} 8x^4-9x^3+12x^2-8\equiv 0 \pmod{2^3}, \\ 8x^4-9x^3+12x^2-8\equiv 0 \pmod{3^2}. \end{cases}$$

$$\Longrightarrow \begin{cases} x^2(x-4)\equiv 0 \pmod{2^3} \\ x^4-3x^2-1\equiv 0 \pmod{3^2} \end{cases} \text{等价。}$$

3. 由同余的性质 5^0，以 $4a$ 同乘（α）的两边及模 m，得

$4a^2x^2+4abx+4ac\equiv 0 \pmod{4am}$.

$\Longrightarrow (2ax+b)^2\equiv b^2-4ac \pmod{4am}$.

令 $y=2ax+b$，$D=b^2-4ac$，则

$$y^2\equiv D \pmod{4am}. \qquad (\beta)$$

若 y_0 是（β）的解，则 $y_0^2\equiv D \pmod{4am} \Longrightarrow (y_0-b)(y_0+b)\equiv -4ac \pmod{4am} \Longrightarrow 4a\mid(y_0-b)(y_0+b)$.

若 $2a\mid y_0-b$，则 $x_0=\frac{y_0-b}{2a}$ 是（α）的一个解，因为此时 $y_0=2ax_0+b$。若 $2a\nmid y_0-b$，则不能从 y_0 导出（α）的解，这与"化成"的意义并不矛盾，但是"化成"指的是（α）的每一个解都可以从（β）的解导出，为此必须再证：若 x_0 是（α）的解，则 $y_0=2ax_0+b$ 是（β）的解。事实上，若 x_0 是（α）的解，则 $ax_0^2+bx_0+c\equiv 0 \pmod m$，用4a乘同余式的两边及模 m，即得 $(2ax_0+b)^2\equiv D \pmod{4am}$，此时 $y_0=2ax_0+b$ 是（β）的解，

也就是（α）的每一个解，在（β）中都有它相对应的解。

4. （i）因为（4，13）=1，原同余式两边同乘以10得

$x^2-6x+9=(x-3)^2\equiv 0\ (\bmod 13) \Longrightarrow y^2\equiv 0\ (\bmod 13)$，

$y=x-3$。

（ii） $(5x)^2+2\times 14\times 5x+14^2\equiv 14^2-80\equiv 116\ (\bmod 225)$

$\Longrightarrow (5x+14)^2\equiv 116\ (\bmod 225) \Longrightarrow y^2\equiv D\ (\bmod 225)$。

其中 $y=5x+14$，$D=116$。

（iii） 同余式两边及模同乘以 3 得

$(6x)^2+2\times 2\times 6x+2^2\equiv 45+4\equiv 49\ (\bmod 132)$

$\Longrightarrow y^2\equiv 49\ (\bmod 132)$，$y=6x+2$。

5. $(\pm 1)\equiv 1$，$(\pm 2)^2\equiv 4$，$(\pm 3)^2\equiv 9$，$(\pm 4)^2\equiv 16$，$(\pm 5)^2\equiv 25$，$(\pm 6)^2\equiv 36$，$(\pm 7)^2\equiv 12$，$(\pm 8)^2\equiv 27$，$(\pm 9)^2\equiv 7$，$(\pm 10)^2\equiv 26$，$(\pm 11)^2\equiv 10$，$(\pm 12)^2\equiv 33$，$(\pm 13)^2\equiv 21$，$(\pm 14)^2\equiv 11$，$(\pm 15)^2\equiv 3$，$(\pm 16)^2\equiv 34$，$(\pm 17)^2\equiv 30$，$(\pm 18)^2\equiv 28\ (\bmod 37)$ 都是模37的平方剩余，而其它18个小于37与37互素的正整数都是模37的平方非剩余。

6. 设 a，b 都是模 p 的平方剩余（或平方非剩余），则

$$\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)=1\ (\text{或}-1) \Longrightarrow \left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)=(\pm 1)^2$$
$$=1.$$

设a，b 一个是模 p 的平方剩余，一个是模 p 的平方非剩余，则

$$\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)=-1.$$

7. $5^{\frac{17-1}{2}}=5^8\equiv -1$，$7^8\equiv -1$，$8^8\equiv 1\ (\bmod 17)$，所以 5，7 是模17的平方非剩余，8 是模17的平方剩余。

8. $1\cdot a\equiv 5$，$2a\equiv -9$，$3a\equiv -4$，$4a\equiv 1$，$5a\equiv 6$，$6a\equiv -8$，$7a\equiv -3$，$8a\equiv 2\ (\bmod 19)$，其中负的个数 $\mu=4$

$$\therefore\ \left(\frac{5}{19}\right)=(-1)^4=1.$$

与用二次反转定律计算的结果是一样的.

9.（i） 若 $x^2 \equiv a \pmod{p^\alpha}$ 有解，则 $x^2 \equiv a \pmod p$ 有解，设其解是：$x \equiv b \pmod p$，即 $b^2 \equiv a \pmod p$，令 $b^2 - a = kp \Longrightarrow (b^2-a)^\alpha = k^\alpha p^\alpha \equiv 0 \pmod{p^\alpha}$，而 $(b+\sqrt{a})^\alpha$

$$= b^\alpha + c_\alpha^1 b^{\alpha-1}\sqrt{a} + c_\alpha^2 b^{\alpha-2} a + c_\alpha^3 b^{\alpha-3} a\sqrt{a} + \cdots + (\sqrt{a})^\alpha$$

$= t + v\sqrt{a}$；

$$(b-\sqrt{a})^\alpha = t - v\sqrt{a}.$$

相加得

$$t = \frac{(b+\sqrt{a})^\alpha + (b-\sqrt{a})^\alpha}{2}$$

是整数，相乘得

$$(b^2-a)^\alpha = t^2 - av^2 \Longrightarrow t^2 - av^2 \equiv 0 \pmod{p^\alpha} \Longrightarrow t^2 \equiv av^2 \pmod{p^\alpha}.$$

（ii） 今证明，$(t, p) = (v, p) = 1$. 令

$$t = \frac{1}{2}[(b+\sqrt{a})^\alpha + (b-\sqrt{a})^\alpha] = f(a, b),$$

显然 $f(a, b)$ 是整数，因为 $b^2 \equiv a \pmod p$，所以

$$t = f(a, b) \equiv f(b^2, b) \pmod p.$$

而当，$a = b^2$ 时，可得

$$t \equiv 2^{\alpha-1} b^\alpha \pmod p$$

又 $(2, p) = (b, p) = 1 \Longrightarrow (t, p) = 1$. $t^2 \equiv av^2 \pmod{p^\alpha}$ $\Longrightarrow t^2 \equiv av^2 \pmod p$，$(t, p) = (a, p) = 1 \Longrightarrow (v, p) = 1$.

（iii） $\because (t, p) = (a, p) = (v, p) = 1$.

$\therefore \quad tu \equiv a \pmod{p^\alpha}$

有解 u（定理4·9），所以

$$t^2u^2 \equiv a^2 \pmod{p^\alpha}.$$

用 u^2 乘 $t^2 \equiv av^2 \pmod{p^\alpha}$ 的两边，即得

$u^2v^2 \equiv a \pmod{p^\alpha}$，

即 $x \equiv \pm uv$ 是 $x^2 \equiv a \pmod{p^\alpha}$ 的两个解。

10. (i) $x^2 \equiv 7 \pmod{3^3}$. $\quad(\alpha)$

因为 $x^2 \equiv 1 \pmod 3$ 有解 $x \equiv \pm 1 \pmod 3$，所以

$(1-\sqrt{7})^3 = 22 - 10\sqrt{7} \Longrightarrow t = 22,\ v = 10$

今解

$22u \equiv 7 \pmod{3^3} \Longrightarrow u \equiv 4 \pmod{27}$.

故 $x \equiv \pm 10 \times 4 \equiv \pm 13 \pmod{27}$ 是 (α) 的解。

(ii) $x^2 \equiv 39 \pmod{5^4}$. $\quad(\beta)$

因为 $x^2 \equiv 4 \pmod 5$ 有解 $x \equiv \pm 2 \pmod 5$，所以

$(2-\sqrt{39})^4 = 2473 - 344\sqrt{39} \Longrightarrow t = 2473,\ v = 344$

今解

$2473u \equiv 39 \pmod{5^4} \Longrightarrow -27u \equiv 39 \pmod{5^4} \Longrightarrow u \equiv 68 \pmod{5^4}$.

故 $x \equiv \pm uv \equiv \pm 344 \times 68 \equiv \pm 267 \pmod{5^4}$ 是 (β) 的两个解。

11. (i) $94 = 2 \times 47$, $\left(\frac{94}{109}\right) = \left(\frac{2}{109}\right)\left(\frac{47}{109}\right)$

$= -\left(\frac{47}{109}\right) = -\left(\frac{109}{47}\right) = -\left(\frac{15}{47}\right) = -\left(\frac{3}{47}\right)\left(\frac{5}{47}\right)$

$= \left(\frac{47}{3}\right)\left(\frac{47}{5}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = 1$.

同样方法可以计算（过程略）(ii) $\left(\frac{111}{271}\right) = -1$,

(iii) $\left(\frac{342}{677}\right) = 1$, (iv) $\left(\frac{93}{131}\right) = -1$,

(v) $\left(\frac{2115}{6269}\right) = 1$.

(vi) $\left(\frac{589}{1283}\right) = \left(\frac{19}{1283}\right)\left(\frac{31}{1283}\right) = \left(\frac{1283}{19}\right)\left(\frac{1283}{31}\right)$

$$=\left(\frac{10}{19}\right)\left(\frac{12}{31}\right)=\left(\frac{2}{19}\right)\left(\frac{5}{19}\right)\left(\frac{2}{31}\right)^2\left(\frac{3}{31}\right)$$

$$=\left(\frac{19}{5}\right)\left(\frac{31}{3}\right)=\left(\frac{4}{5}\right)\left(\frac{1}{3}\right)=1.$$

12. (i) $\left(\frac{47}{125}\right)=\left(\frac{125}{47}\right)=\left(\frac{5}{47}\right)=\left(\frac{47}{5}\right)=\left(\frac{2}{5}\right)$

$=-1$。

(ii) $\left(\frac{5610}{6649}\right)=\left(\frac{2}{6649}\right)\left(\frac{3}{6649}\right)\left(\frac{5}{6649}\right)$

$\times\left(\frac{11}{6649}\right)\left(\frac{17}{6649}\right)=\left(\frac{1}{3}\right)\left(\frac{4}{5}\right)\left(\frac{5}{11}\right)$

$\times\left(\frac{2}{17}\right)=\left(\frac{11}{5}\right)=1$.

同样方法可以计算（略）(iii) $\left(\frac{131}{283}\right)=-1$,

(iv) $\left(\frac{116}{397}\right)=1$, (v) $\left(\frac{328}{625}\right)=1$.

13. 略

14. (i) 因为 $\left(\frac{429}{563}\right)=1$，故有解。

(ii) $\left(\frac{680}{769}\right)=1$，有解。

(iii) $\left(\frac{503}{1013}\right)=1$，有解。

15. $\left(\frac{-2}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)=(-1)^{\frac{p-1}{2}+\frac{p^2-1}{8}}$，故

-2为 p 的平方剩余时，必 $\frac{p-1}{2}+\frac{p^2-1}{8}=2n$.

(i) $p=4k+1$ 且 $p=8k'\pm1$，即 $p=8m+1$;

(ii) $p=4k+3$ 且 $p=8k'\pm3$，即 $p=8m+3$.

-2为模 p 的平方非剩余时，必 $\frac{p-1}{2}+\frac{p^2-1}{8}=2n+1$.

(i) $p=4k+3$ 且 $p=8k'\pm1$，即 $p=8m+7$;

(ii) $p=4k+1$ 且 $p=8k'\pm3$，即 $p=8m+5$。

16. 由欧拉判别条件知，当 $p=8n+7$ 时，有

$$2^{\frac{p-1}{2}}\equiv\left(\frac{2}{p}\right)(\bmod p)\Longrightarrow 2^{4n+3}\equiv\left(\frac{2}{8n+7}\right)$$

$$=1(\bmod 8n+7)。$$

而$23=8\times2+7$，$47=8\times5+7$，$503=8\times62+7$都是形如$8n+7$的素数，并且$11=\frac{23-1}{2}$，$23=\frac{47-1}{2}$，$251=\frac{503-1}{2}$，所以

$23\mid 2^{11}-1$，$47\mid 2^{23}-1$，$503\mid 2^{251}-1$。

17. 若 $p=4k+1$，则$\left(\frac{3}{p}\right)=\left(\frac{p}{3}\right)$，分别讨论：

(i) $k=3m$ 时，$\left(\frac{p}{3}\right)=\left(\frac{1}{3}\right)=1$，即$\left(\frac{3}{12m+1}\right)=1$；

(ii) $k=3m+1$ 时，$p=12m+5$，$\left(\frac{p}{3}\right)=\left(\frac{2}{3}\right)=-1$；

(iii) $k=3m+2$时，$p=12m+9$ 不是素数，故不存在这种情况。

此时$\left(\frac{-3}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)=\left(\frac{3}{p}\right)$。

若 $p=4m+3$，则$\left(\frac{3}{p}\right)=-\left(\frac{p}{3}\right)$分别讨论：

(i) $k=3m$，$p=12m+3$ 是合数，故不可能；

(ii) $k=3m+1$，$p=12m+7$，$-\left(\frac{p}{3}\right)=-\left(\frac{1}{3}\right)=-1$，即$\left(\frac{3}{p}\right)=-1$；

(iii) $k=3m+2$，$p=12m+11$，$-\left(\frac{p}{3}\right)=-\left(\frac{2}{3}\right)=1$。即$\left(\frac{3}{p}\right)=1$。

此时$\left(\frac{-3}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)=-\left(\frac{3}{p}\right)$。

所以，当 p 是形如$12m\pm1$的素数时，3 是模 p 的平方剩余；当 p 是形如$12m+1$，$12m+7$时，-3是模 p 的平方剩余。

当 p 是形如$12m\pm5$的素数时，3 是 p 的平方非剩余；当 p 是形如$12m+5$，$12m-1$时，-3是 p 的平方非剩余。

18. 3 是形如$24m+5$，$24m+17$，$24m+7$，$24m+19$的素数的平方非剩余，对 2 来说

$$\left(\frac{2}{24m+5}\right)=-1,\ \left(\frac{2}{24m+17}\right)=1,\ \left(\frac{2}{24m+7}\right)=1,$$

$$\left(\frac{2}{24m+19}\right)=-1$$

故 p 为形如$24m+7$和$24m+17$的素数时，3 是它的最小平方非剩余。

19. $\because \left(\frac{p-a}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{a}{p}\right)=(-1)^{\frac{p-1}{2}}\left(\frac{a}{p}\right)$

$$\Longrightarrow \left(\frac{p-a}{p}\right)=\begin{cases}\left(\frac{a}{p}\right), & \text{当}p=4k+1\text{时},\\ -\left(\frac{a}{p}\right), & \text{当}p=4k+3\text{时},\end{cases}$$

20. 若 $x^2-a\equiv0\pmod p$有解，则$\left(\frac{a}{p}\right)=1$，当$(u,p)=1$时，$\left(\frac{au^2}{p}\right)=\left(\frac{a}{p}\right)=1$. 则$t^2-au^2\equiv0\pmod p$有解 t。

当 $p|u$ 时，取 $t\equiv0\pmod p$，则 $t^2-au^2\equiv0\pmod p$。也就是说，当 $p|x^2-a$ 时，任给 u 都存在 t，使得 $p|t^2-au^2$。

若$(t,u)=1$，且$t^2-au^2\equiv0\pmod p$，则$(p,u)=1$。否则$p|u\Longrightarrow p|t$，这与$(t,u)=1$矛盾，于是

$\exists v \ni uv\equiv1\pmod p\Longrightarrow(tv)^2-a\equiv0\pmod p$

$\Longrightarrow x\equiv tv\pmod p$ 是$x^2-a\equiv0\pmod p$的解。

也就是说，当 $p|t^2-au^2$，$(t,u)=1$时，则存在 v 使得，当$x\equiv tv\pmod p$时，$p|x^2-a$.

21. (i)由前题知道(i)与x^2-3有同样的素约数。又由第17

题知道形如$12m\pm1$的素数p，都有$\left(\frac{3}{p}\right)=1$，故$p|t^2-3u^2$。此外还有$2|t^2-3u^2$，$3|t^2-3u^2$。因为$x^2\equiv3 \pmod 2$及$x^2\equiv0 \pmod 3$有解。

(ii) 同理t^2+7u^2与x^2+7有同样的素约数。因为$x^2\equiv-7 \pmod p$，当$p=2$，7时有解。当$p=4k+1$时，$\left(\frac{-7}{p}\right)=\left(\frac{p}{7}\right)$；当$p=4k+3$时，$\left(\frac{-7}{p}\right)=\left(\frac{p}{7}\right)$。下面分别讨论，形如$28k\pm1$，$28k\pm3$，$28k\pm5$，$28k\pm9$，$28k\pm11$，$28k\pm13$的素数是否$-7$的平方剩余。

$$\because\quad \left(\frac{-1}{28k\pm1}\right)=\pm1;\quad \left(\frac{-1}{28k\pm3}\right)=\mp1;$$

$$\left(\frac{-1}{28k\pm5}\right)=\pm1;\quad \left(\frac{-1}{28k\pm9}\right)=\pm1.$$

$$\therefore\quad \left(\frac{-7}{28k\pm1}\right)=\pm\left(\frac{7}{28k\pm1}\right)=\left(\frac{28k\pm1}{7}\right)=\pm1;$$

$$\left(\frac{-7}{28k\pm3}\right)=\mp\left(\frac{7}{28k\pm3}\right)=\left(\frac{28k\pm3}{7}\right)=\left(\frac{\pm3}{7}\right)$$
$$=\mp1;$$

$$\left(\frac{-7}{28k\pm5}\right)=\pm\left(\frac{7}{28k\pm5}\right)=\left(\frac{28k\pm5}{7}\right)=\left(\frac{\mp2}{7}\right)$$
$$=\mp1;$$

$$\left(\frac{-7}{28k\pm9}\right)=\pm\left(\frac{7}{28k\pm9}\right)=\left(\frac{\pm2}{7}\right)=\pm1.$$

$$\left(\frac{-7}{28k\pm11}\right)=\left(\frac{28k\pm11}{7}\right)=\left(\frac{\pm4}{7}\right)=\pm1;$$

$$\left(\frac{-7}{28\pm13}\right)=\left(\frac{28k\pm13}{7}\right)=\left(\frac{\mp1}{7}\right)=\mp1.$$

所以p为形如$28k+1$，$28k-3$，$28k-5$，$28k+9$，$28k+11$，$28k$

-13的素数时，$p|t^2+7u^2$，以及$2|t^2+7u^2$，$7|t^2+7u^2$*.

(iii) $x^2\equiv7(\bmod p)$，当$p=2$，7时有解，所以$2|t^2-7u^2$，$7|t^2-7u^2$。此外把(ii)的演算过程中用7代替-7，可以看到：p为形如$28k\pm1$，$28k\pm3$，$28k\pm9$的素数时，$p|t^2-7u^2$。

(iv) 显然$2|t^2-14u^2$，$7|t^2-14u^2$。此外研究形如$56\pm a$的素数p，其中a是不大于27且不含7的因数的奇数，14是否p的平方剩余。

仿照(ii)的方法计算结果是：

$$\left(\frac{14}{56k\pm1}\right)=1;\quad \left(\frac{14}{56k\pm3}\right)=-1;\quad \left(\frac{14}{56k\pm5}=1;\right)$$

$$\left(\frac{14}{56k\pm9}\right)=1;\quad \left(\frac{14}{56k\pm11}\right)=1;\quad \left(\frac{14}{56k\pm13}\right)=1;$$

$$\left(\frac{14}{56k\pm15}\right)=-1;\left(\frac{4}{56k\pm17}\right)=-1;\quad \left(\frac{14}{56k\pm19}\right)=-1;$$

$$\left(\frac{14}{56k\pm23}\right)=-1,\quad \left(\frac{14}{56k\pm25}\right)=1,\quad \left(\frac{14}{56k\pm27}\right)=-1.$$

所以t^2-14u^2有2，7以及形如$56k\pm1$，$56k\pm5$，$56k\pm9$，$56k\pm11$，$56k\pm13$，$56k\pm25$的素约数。

(v) 显然$2|t^2-5u^2$，$5|t^2-5u^2$。此外研究$20k\pm1$，$20k\pm3$，$20k\pm7$，$20k\pm9$的素数p。知道

$$\left(\frac{5}{20k\pm1}\right)=1,\quad \left(\frac{5}{20k\pm3}\right)=-1,\quad \left(\frac{5}{20k\pm7}\right)=-1,$$

$$\left(\frac{5}{20k\pm9}\right)=1.$$

所以2，5以及形如$20k\pm1$，$20k\pm9$的素数都是t^2-5u^2的约数。

22. (i) $313=2^3\times39+1$，$\lambda=3$，$k=39$

$a^k=11^{39}=(11^3)^{13}\equiv(79)^{13}\equiv(64)^4\cdot79\equiv-1(\bmod 313)$.

---

* 注意：若用$14k\pm a$来讨论，则

$$\left(\frac{-7}{14k+1}\right)=(-1)^{7k}\left(\frac{7}{14k+1}\right)=\begin{cases}\left(\frac{7}{14k+1}\right)，当k为偶数时；\\ -\left(\frac{7}{14k+1}\right)，当k为奇数时。\end{cases}$$

故仍应转化为$28k\pm a$形来讨论。

又因$\left(\frac{5}{313}\right)=\left(\frac{3}{5}\right)=\left(\frac{2}{3}\right)=-1$，取 $f=5$，故原同余式的解是

$$x\equiv\pm f^{2^{\lambda}-2^{k}}a^{\frac{k+1}{2}}=\pm 5^{2\times 39}11^{20}(\bmod 313)$$ 而 $25^2\equiv-1$，

$25^4\equiv1$，$25^{36}\equiv1$，$25^3\equiv-25(\bmod 313)\Longrightarrow 5^{2\times 39}\equiv-25\ (\bmod 313)$；

$11^{20}\equiv(-10)^6\equiv137(\bmod 313)$。

$\therefore\quad x\equiv\pm((-25)\times137)\equiv\pm18(\bmod 313)$

(ii) $641=2^7\times5+1$，$\lambda=7$，$k=5$；

$a^k=8^5\equiv250\times8\equiv77(\bmod 641)$；

因$\left(\frac{3}{641}\right)=-1$，故取 $f=3$。解

$$z^2\equiv-1,\ z_2^{2^2}\equiv-1,\ z_3^{2^3}\equiv-1, z_4^{2^4}\equiv-1, z_5^{2^5}\equiv-1,\ z_6^{2^6}\equiv-1\quad(\bmod 641)\qquad(1)$$

得对模641)的

$u_{1,1}=3^{2^5\times5}=243^{2^5}\equiv77^{2^4}\equiv160^{2^3}\equiv(-40)^{2^2}\equiv318^2\equiv$

$\equiv-154$，$u_{12}\equiv-154$。

$u_{2,1}\equiv3^{2^4\cdot5}\equiv318$，$u_{2,2}\equiv-318$，$u_{2,3}\equiv-154\times318$

$\equiv-256$，$u_{2,4}\equiv256$。

$u_{3,1}\equiv-40$，$u_{3,2}\equiv40$，$u_{3,3}\equiv-250$，$u_{3,4}\equiv250$，

$u_{3,5}\equiv-59$，$u_{3,6}\equiv59$，$u_{3,7}\equiv258$，$u_{3,8}\equiv-258$。

$u_{4,1}\equiv160$，$u_{4,2}\equiv-160$，$u_{4,3}\equiv-282$，$u_{4,4}\equiv282$，

$u_{4,5}\equiv-236$，$u_{4,6}\equiv236$，$u_{4,7}\equiv202$，$u_{4,8}\equiv-202$，

$u_{4,9}\equiv-10$，$u_{4,10}\equiv10$，$u_{4,11}\equiv308$，$u_{4,12}\equiv-308$，…。

$u_{5,1}\equiv77$，$u_{5,2}\equiv-77$，…。

因为$u_{5,1}\equiv77\equiv a^k(\bmod 641)$，它是(1)的第五个同余式的解。今求$a^k\equiv b^2(\bmod 641)$的b。

$u_{6,1}\equiv243$，$u_{6,2}\equiv-243(\bmod 641)$，而 $u_{6,1}^2=59049\equiv77(\bmod 641)$，故$b=243$。

次解 $bt \equiv 1 \pmod{641}$，解得$t \equiv 153 \pmod{641}$。

$$\therefore \quad x \equiv \pm a^{\frac{k+1}{2}} t \equiv \pm 8^3 \times 153 \equiv \mp 134 \pmod{641}.$$

注意：上面是此题的一般解法．但是此题情况比较特殊，因为 $b = u_{6,1}$故无须再求$u_{6,3}$，…，$u_{6,4}$，且$a^k \equiv 77 \equiv u_{5,1}$，因而$u_{2,1}$开始的计算亦属多余．故到(1)式为止，下面可简解于下：

$$u_{1,1} = 3^{2^5 \cdot 5} = 243^{2^5} \equiv 77^{2^4} \equiv 160^{2^3} = (-40)^{2^2} \equiv 318^2$$
$$\equiv -154 \pmod{641}.$$

从而知道，对模641，有

$u_{2,1} \equiv 318$，$u_{3,1} \equiv -40$，$u_{4,1} \equiv 160$，$u_{5,1} \equiv 77 \equiv a^k$，

$u_{6,1} \equiv 243$． 而且 $u_{6,1}^2 \equiv 243^2 \equiv 77 \equiv a^k$．

所以$b = 243$，今解$bt \equiv 1 \pmod{641}$ 得$t = 153$，故原同余式的解是：

$$x \equiv \pm a^{\frac{k+1}{2}} t \equiv \pm 8^3 \times 153 \equiv \mp 134 \pmod{641}.$$

23．(i) $x^2 \equiv 24 \pmod{5^3}$． (1)

$b^2 \equiv 4 \pmod 5 \Longrightarrow b \equiv \pm 2 \pmod 5$．

$(2 - \sqrt{24})^3 = 152 - 36\sqrt{24}$．

$\therefore \quad t = 152, \quad v = 36$．

$tu \equiv a \pmod{p^\alpha}$ 即 $27u \equiv 24 \pmod{5^3}$

解得 $u \equiv -13 \pmod{125}$．故(1)的解是

$x \equiv \mp 13 \times 36 \equiv \pm 32 \pmod{125}$．

(ii) $x^2 \equiv 18 \pmod{7^3}$． (2)

$b^2 \equiv 4 \pmod 7 \Longrightarrow b \equiv \pm 2 \pmod 7$．

$(2 - \sqrt{18})^3 = 116 - 30\sqrt{18} \Longrightarrow t = 116, \quad v = 30$

解

$116u \equiv 18 \pmod{343} \Longrightarrow 58u \equiv 9 \pmod{343}$

$\Longrightarrow u \equiv 195 \pmod{343}$．

$\therefore \quad x \equiv \pm 30 \times 195 \equiv \pm 19 \pmod{343}$．

是（2）的解。

(iii) $x^2 \equiv 13 \pmod{3^5}$ **(3)**

$b^2 \equiv 1 \pmod 3 \Longrightarrow b \equiv \pm 1 \pmod 3$,

$(1-\sqrt{13})^5 = 976 - 304\sqrt{13} \Longrightarrow t = 976$, $v = 304$.

解

$tu \equiv 13 \equiv \pmod{3^5} \Longrightarrow 976u \equiv 13 \pmod{3^5}$

$\Longrightarrow u \equiv 64 \pmod{3^5}$.

∴ $x \equiv \pm uv \equiv \pm 304 \times 64 \equiv \pm 16 \pmod{243}$

是（3）的解。

24. (i) $x^2 \equiv 57 \pmod{2^9}$ **(1)**

因为$57 \equiv 1 \pmod 8$，所以由定理5·7知同余式（1）有解，且有四个解。把它写成

$$x = \pm(1+4t_3)$$

代入（1）的左边得

$(1+4t_3)^2 \equiv 57 \pmod{16} \Longrightarrow t_3 \equiv 1 \pmod 2$,

∴ $x = \pm(1+4(1+2t_4)) = \pm(5+8t_4)$

是适合$x^2 \equiv 57 \pmod{16}$的一切整数解。再代入（1）的左边得

$(5+8t_4)^2 \equiv 57 \pmod{32} \Longrightarrow t_4 \equiv 0 \pmod 2$,

∴ $x = \pm(5+8\times 2t_5) = \pm(5+16t_5)$

是$x^2 \equiv 57 \pmod{32}$的一切整数解。仿此由 $(5+16t_5)^2 \equiv 57 \pmod{64}$ 解得$t_5 \equiv 1 \pmod 2$，故$x = \pm[5+16(1+2t_6)] = \pm(21+32t_6)$是$x^2 \equiv 56 \pmod{64}$的一切整数解。又由$(21+32t_6)^2 \equiv 57 \pmod{128}$解得$t_6 \equiv 0 \pmod 2$，故$x = \pm(21+64t_7)$是$x^2 \equiv 57 \pmod{128}$的一切整数解。由$(21+64t_7)^2 \equiv 57 \pmod{256}$解得$t_7 \equiv 1 \pmod 2$，故$x = \pm(85+128t_8)$是$x^2 \equiv 57 \pmod{256}$的一切整数解。由$(85+128t_8)^2 \equiv 57 \pmod{512}$解得$t_8 \equiv 0 \pmod 2$，故$x = \pm(85+256t_9)$是（1）的一切解。即

$x \equiv \pm 85$，± 341，或$x \equiv \pm 85$，$\pm 171 \pmod{2^9}$是（1）的四个解。

仿照上面方法可解：(ii)$x^2 \equiv 41 \pmod{2^{10}}$得$x \equiv \pm 205$，$\pm 307$；(iii)$x^2 \equiv 17 \pmod{2^{14}}$得$x \equiv 1769$，$\pm 6423 \pmod{2^{14}}$（略）

25. 当$\alpha = 2^{\beta}$为偶数时，$\left[\frac{\alpha}{2}\right] = \beta$，则$p^{\left[\frac{\alpha}{2}\right]} = p^{\beta}$，而同余式

$x^2 \equiv 0 (\bmod p^{\alpha})$有解

$x \equiv 0, p^{\beta}, 2p^{\beta}, \cdots, (p^{\beta-1}) p^{\beta} (\bmod p^{\alpha})$，故其解的个数共有

$p^{\beta} = p^{\left[\frac{\alpha}{2}\right]}$.

当$\alpha = \alpha\beta + 1$为奇数时，$p^{\left[\frac{\alpha}{2}\right]} = p^{\beta}$，而$x^2 \equiv 0 (\bmod p^{\alpha})$有解

$x \equiv 0, p^{\beta+1}, 2p^{\beta+1}, \cdots, (p^{\beta-1}) p^{\beta+1} (\bmod p^{\beta})$，共有$p^{\beta} = p^{\left[\frac{\alpha}{2}\right]}$个解。

26. 应用前题证明的过程，得

(i) $x^2 \equiv 0 (\bmod 5^4)$有解

$x \equiv 0, 5^2, 2 \cdot 5^2, 3 \cdot 5^2, \cdots, 24 \cdot 5^2 (\bmod 5^4)$

(ii) $x^2 \equiv 0 (\bmod 11^2)$有解

$x \equiv 0, 11^2, 2 \cdot 11^2, \cdots, 10 \times 11^2 (\bmod 11^3)$.

27. (i) $x^2 \equiv 34 (\bmod 9 \times 5 \times 11)$等价于

$$\begin{cases} x^2 \equiv 34 (\bmod 3^2), \\ x^2 \equiv 34 (\bmod 5), \\ x^2 \equiv 34 (\bmod 11). \end{cases} \cong \begin{cases} x^2 \equiv 7 (\bmod 9) \\ x^2 \equiv 4 (\bmod 5), \\ x^2 \equiv 1 (\bmod 11). \end{cases}$$

从观察可得第1，2，3个同余式依次有解：± 4，± 2，± 1. 由孙子定理，$M = 495$，$M_1' M_1 = 55$，$M_2' M_2 = -99$，$M_3 M_3 = 45$. 故原同余式的解

$x \equiv b_1 \times 55 + b_2 \times (-99) + b \times 45 (\bmod 495)$

计算得$x \equiv \pm 67$，± 32，± 23，± 122等八个解。

(ii) $x^2 \equiv 48 (\bmod 416)$等价于

$$\begin{cases} x^2 \equiv 48 (\bmod 2^5), \\ x^2 \equiv 48 (\bmod 13). \end{cases} \cong \begin{cases} x^2 \equiv 16 (\bmod 2^5), \\ x^2 \equiv 9 (\bmod 13). \end{cases}$$

同(i)的方法，解得$x \equiv \pm 36$，± 68，± 140，$\pm 172 (\bmod 416)$.

28. (i) 原同余式等价于

$$\begin{cases} 8x^2 + 15x - 6 \equiv 0 (\bmod 2^3), \\ 8x^2 + 15x - 60 \equiv (\bmod 7). \end{cases} \cong \begin{cases} 7x - 6 \equiv 0 (\bmod 8), \\ x^2 + x + 1 \equiv 0 (\bmod 7). \end{cases}$$

$$\cong \begin{cases} 7x-60\equiv(\bmod 8), \\ (2x+1)^2+3\equiv 0(\bmod 7). \end{cases} \cong \begin{cases} x\equiv 2(\bmod 8) \\ x\equiv 4,\ 2(\bmod 7) \end{cases}$$

用孙子定理解得 $x\equiv 2,\ 18(\bmod 56)$.

29. (i) 必要性：若(a)有正整数解，则$(x, p)=(y, p)=1$，于是∃正整数y_1∋$yy'\equiv 1(\bmod p)$，$(y', p)=1$。所以

$$(x^2+3y^2)y_1^2\equiv(xy')^2+3\equiv 0(\bmod p)$$

有解。即$\left(\frac{-3}{p}\right)=1$。

(ii) 充分性：若$\left(\frac{-3}{p}\right)=1$，则$x^2+3\equiv 0\ (\bmod p)$有解，若$p=3$，(a)转化为$x^2\equiv 0(\bmod 3)$有解$x\equiv 0(\bmod 3)$.故设$p>3$，$x^2+3\equiv 0(\bmod p)$有解$|x|<\frac{p}{2}$时，

$$0<3+x^2<3+\frac{p^2}{4}<p^2,$$

故存在正整数m，x，y，使得

$$x^2+3y^2=mp,\quad 0<m<p \tag{b}$$

成立〔因若$x_0(0<x_0<p)$是$x^2+3\equiv 0(\bmod p)$的解，则$x_0^2+3=sp$ $(0<s<p)$，此时$y=1$，$x=x_0$，$m=s$〕。设m_0是使(b)成立的最小正整数，下面证明$m_0=1$。

若$m_0>1$，由绝对最小剩余系的性质，立即知道存在有二整数x_1，y_1，使得

$$x\equiv x_1,\quad y\equiv y_1(\bmod m_0),\quad |x_1|\leqslant\frac{1}{2}m_0,\quad |y_1|\leqslant\frac{1}{2}m_0 \tag{c}$$

并且$|x_1|$，$|y_1|$不全为0，否则$x_1=y_1=0\Longrightarrow m_0|x$，$m_0|y\Longrightarrow m_0^2|x^2+3y^2\Longrightarrow m_0^2|m_0p\Longrightarrow m_0|p$，但$m_0<p$，于是$m_0=1$这与$m_0>1$的假设矛盾。

由(c)即得

$$0<x_1^2+3y_1^2\leqslant\left(\frac{1}{4}+\frac{3}{4}\right)m_0^2=m_0^2,$$

$$x_1^2+3y_1^2\equiv x^2+3y^2=m_0p\equiv 0(\bmod m_0),$$

$\therefore \quad x_1^2+3y_1^2=m_1m_0,\ 0<m_1\leqslant m_0,$ (d)

其中$m_1\neq m_0$。否则，$|x_1|=|y_1|=\frac{1}{2}m_0\Longrightarrow|x|=|y|=\frac{1}{2}m_0$(若$|x|=km_0+\frac{1}{2}m_0$，$|y|=hm_0+\frac{1}{2}m_0$，$k\geqslant0$，$h\geqslant0$，则$x^2+3y^2=(1+k+k^2+3h+3h^2)m_0^2\Longrightarrow m_0|p$与$1<m_0<p$矛盾)所以$m_1<m_0$，由(c)及(d)得

$$m_0^2m_1p=(x^2+3y^2)(x_1^2+3y_1^2)=(xx_1+3yy_1)^2+3(xy_1-x_1y)^2 \tag{e}$$

又由(c)得

$$\begin{cases}xx_1+3yy_1\equiv x_1^2+3y_1^2\equiv0\pmod{m_0},\\ xy_1-x_1y\equiv x_1y_1-x_1y_1\equiv0\pmod{m_0}.\end{cases} \tag{f}$$

由(f)及(e)知道不定方程

$$X^2+3Y^2=m_1p$$

有非负整数解

$$X=\frac{|xx_1+3yy_1|}{m_0},\quad Y=\frac{|xy_1-x_1y|}{m_0}$$

且$X\neq0$，$Y\neq0$，否则m_1p是一个数的平方或一个数平方的三倍，由于$0<m_1<p$，p是素数，故这是不可能的。从而得到m_1也是使(b)成立的正整数，这与m_0的最小性矛盾，故$m_0=1$。这就证明了本题的结论。

30. 由拉格朗日定理（定理5·13）知道$g(2)=4$，而$G(2)\leqslant g(2)=4$。只要证$G(2)\geqslant4$就可以了。显然$G(2)\neq1$，$G(2)\neq2$，我们只须证$G(2)\neq3$就可以了。

若$G(2)=3$，则存在N，当$n>N$时，n可以表成三个非负整数的平方和。

当整数$m>\frac{N-7}{8}$时，则$8m+7>N$，所以$8m+7$可表示成三个非负整数的平方和。设

$$8m+7=x^2+y^2+z^2\Longrightarrow x^2+y^2+z^2\equiv7\pmod 8$$

由于任何整数x，必$x^2\equiv 0, 1, 4 \pmod 8$之一。所以对于任何整数x，y，z有$x^2+y^2+z^2\not\equiv 7 \pmod 8$（因为0，1，4可重复地任取三数之和不同余于7模8）。这与假设矛盾，故$G(2)\geqslant 4$。

$\therefore\quad G(2)=4$。

第六章　习题解答

1．(i)　因为$2^2\equiv 4$，$2^4\equiv 1 \pmod 5$，所以$2\in_5 4$；同理$3\in_5 4$；$4^2\equiv 1 \pmod 5$，故$4\in_5 2$；$1\in_5 1$。

(ii)　显然$3\in_8 2$，$7\in_8 2$，$5\in_8 2$，$1\in_8 1$。

(iii)　$\varphi(10)=4$，δ只能是1，2，4之一，经验算知，$1\in_{10}1$，$3\in_{10}4$，$7\in_{10}4$，$9\in_{10}2$。

(iv)　$\varphi(11)=10$，δ只能是1，2，5，10之一，而$1\in_{11}1$，而$2^2\equiv 4$，$2^5\equiv -1$，$2^{10}\equiv 1\Longrightarrow 2\in_{11}10$，同理，$3\in_{11}5$，$4\in_{11}5$，$5\in_{11}5$，$6\in_{11}10$，$7\in_{11}10$，$8\in_{11}10$，$9\in_{11}5$，$10\in_{11}2$。

(v)　$\varphi(24)=8$，故δ只能是1，2，4，8之一，经验证知，除$1\in_{24}1$之外，5，7，11，13，17，19，23对于模24都属于方次数2。

2．(i)　若奇素数q使$a^p\equiv 1 \pmod q$，则a对模q所属的方次数δ只能是1或p之一。若$\delta=1$，则$q\mid a-1$；若$\delta=p$，$\varphi(q)=q-1$，而$p\mid\varphi(q)$，又$q-1$是偶数，故$q-1=2px\Longrightarrow q=2px+1$（x是正整数）。

(ii)　若奇素数q使$a^p\equiv -1 (\bmod\ )$，则$a^{2p}\equiv 1 (\bmod q$，所以a对模q所属的方次数δ只能是1，2，p，2p之一。因为$a^p\equiv -1 \pmod q$，所以$\delta\neq 1$且$\delta\neq p$。若$\delta=2$，则$a^2\equiv 1 \pmod q$而$a\not\equiv 1 \pmod q\Longrightarrow a\equiv -1 \pmod q\Longrightarrow q\mid a+1$；若$\delta=2p\Longrightarrow 2p\mid q-1\Longrightarrow q-1=2px\Longrightarrow q=2px+1$（x是正整数）。

3．　由于$a^p-1=(a-1)(a^{p-1}+a^{p-2}+\cdots+1)$，故由前题知道，当p是奇素数时$a^p-1$必有形如$2px+1$的素约数。今设形如$2px+1$的素数只有k个：$p_1$，$p_2$，…，$p_k$则$p_i\nmid (p_1\cdots p_k)^p-1 (i=1,$

2，…，k)，p 为奇素数，所以 $(p_1\cdots p_k)^p-1$ 有不同于 $p_i=1$，…，k，)的素约数。由前题知道它必有不等于 p_i 的 $2px+1$ 形的素约数。

4. 若素数 $q|2^{2^n}+1$，即 $2^{2^n}+1\equiv0(\mathrm{mod}\ q)$，此时 q 必为奇素数。把 $2^{2^n}\equiv-1(\mathrm{mod}\ q)$ 的两边平方得 $2^{2^{n+1}}\equiv1(\mathrm{mod}\ q)$，所以 $2\in_q 2^{n+1}$。而 $\varphi(q)=q-1\Longrightarrow 2^{n+1}|q-1\Longrightarrow q=2^{n+1}x+1$（x 是正整数）。

5. 因为 a 对模 a^n-1 属于方次数 n，所以 $n|\varphi(a^n-1)$。

6. 设 $(\lambda,\ \delta)=d$，$\lambda=\lambda_1 d$，$\delta=\delta_1 d$，而 $a^{\delta}\equiv1(\mathrm{mod}\ m)$，所以

$(a)^{\lambda\frac{\delta}{d}}=(a^{\lambda})^{\delta_1}\equiv1(\mathrm{mod}\ m)$。今证明

$$a^{\lambda}\in_m\frac{\delta}{d}.$$

若有 $(a^{\lambda})^k\equiv1(\mathrm{mod}\ m)$ 则由定理6·2知

$\delta|\lambda k\Longrightarrow\lambda k=\delta h\Longrightarrow\lambda_1 k=\delta_1 h$，$(\lambda_1\delta_1)=1\Longrightarrow\delta_1|k\Longrightarrow$

$a^{\lambda}\in_m\delta_1\Longrightarrow a^{\lambda}\in_m\frac{\delta}{d}$.

7. (i) 7 的原根个数有 $\varphi(6)=2$。经计算知3，5是模 7 的原根。

(ii) 经计算知模17的原根有 3，5，6，7，10，11，12，14等。$\varphi(16)=8$个（演算略）。

(iii) 因 3 是模 7 的原根，由定理6·6

$$(3+7t)^6=1+7(T_0-3^5t+7T)=1+7u,$$

$\therefore$ $u\equiv T_0-3^5t(\mathrm{mod}\ 7)$，$(3^5,\ 7)=1$，$T_0=104$。

而 $3^5t\equiv104\equiv-1(\mathrm{mod}\ 7)$ 即 $5t\equiv-1(\mathrm{mod}\ 7)$，有且只有一个解。$t\equiv4(\mathrm{mod}\ 7)$，所以 t=0，1，2，3，5，6 时，$u\not\equiv0(\mathrm{mod}\ 7)$。因而 3，10，17，24，38，45 都是模49的原根。

又 5 是模 7 的另一个原根。$5^6=15625=1+7\times2232$，$T_0=2232\equiv-1(\mathrm{mod}\ 7)$，$5^5t\equiv-1(\mathrm{mod}\ 7)$ 即 $3t\equiv-1(\mathrm{mod}\ 7)$ 有且只有一个解 $t\equiv2(\mathrm{mod}\ 7)$。所以 t=0，1，3，4，5，6 时，$u\not\equiv0(\mathrm{mod}\ 7)$，因而 5，12，26，33，40，47都是模49的原根。

(iv) 由(i)知2，3是模 5 的原根。$125=5^3$，由定理6·6，$2^4=16=1+3\times5$，$T_0=3$，$2^3t\equiv3 \pmod 5$有且只有一个解 $t\equiv1 \pmod 5$，所以$t=0$，2，3，4；5，7，8，9；10，12，13，14；15，17，18，19；20，22，23，24，时，$u\not\equiv0 \pmod 5$。因而 2，12，17，22；27，37，42，47；52，62，67，72；77，87，92，97；102，112，117，122都是模125的原根。

又$3^4=81=1+16\times5$，$T_0=16$，$3^3t\equiv16 \pmod 5 \Longrightarrow 2t\equiv1 \pmod 5 \Longrightarrow t\equiv3 \pmod 5$，所以$t=0$，1，2，4；5，6，7，9；10，11，12，14；15，16，17，19；20，21，22，24时，$u\in0 \pmod 5$，因而 3，8，13，23；28，33，38，48；53，58，63，73；78，83，88，98；103，108，113，123都是模125的原根。

(v) $81=3^4$，2 是模3的原根，$2^2=4=1+1\times3$，$T_0=1$，$2t-1\equiv0 \pmod 3 \Longrightarrow t\equiv2 \pmod 3$，所以 $t=0$，1；3，4；6，7；9，10；12，13；15，16；18，19；21，22；24，25时，$u\equiv0 \pmod 3$ 因而 2，5；11，14；20，23；29，32；38，41；47，50；56，59；65，68；74，77都是模81的原根。

(vi) $14=2\times7$，7 有原根 3，5；由定理6·7，3+7 与 3，5+7 与 5 之间 3，5 是奇数，故3,5是模14的原根。

(vii) $50=2\times5^2$，由(iv)知道模5^2有原根2,12，17，22及3，8，13，23，所以模50有原根27，37，17，47；3，33，13，23。

8. 因为$\frac{b}{a}$指的是 $$ax\equiv b \pmod m \tag{1}$$
的解 x，(1)的两边取指数得

$$\text{ind } a+\text{ind} x\equiv\text{ind } b \pmod{\varphi(m)},$$

$$\therefore \quad \text{ind}\frac{b}{a}=\text{ind } b-\text{ind } a .$$

9. 设 g 是模m的原根$g^{\varphi(m)}-1=(g^{\frac{1}{2}\varphi(m)}-1)$

$\cdot(g^{\frac{1}{2}\varphi(m)}+1)\equiv0 \pmod m$。

(i)若$m=p^{\alpha}$（p 是奇素数），因为（1）中二因子之差等于 2，所以p不能同时整除此二因子，于是 p^{α} 能且只能整除此二因子之一，又因 g 是模 p^{α} 的原根，故$p^{\alpha} \nmid g^{\frac{1}{2}\varphi(m)}-1$)。

$$\therefore p^{\alpha} \mid g^{\frac{1}{2}\varphi(m)}+1 \Longrightarrow g^{\frac{1}{2}\varphi(m)} \equiv -1\ (\bmod p^{\alpha})$$

$$\Longrightarrow \mathrm{imd}(-1) \equiv \frac{1}{2}\varphi(m)\ (\bmod \varphi(m))。$$

(ii) 若$m=2p^{\alpha}$，g 是$2p^{\alpha}$的原根，则 g 是奇数，且

$p^{\alpha} \nmid g^{\frac{1}{2}\varphi(m)}-1$，则

$$p^{\alpha} \mid g^{\frac{1}{2}\varphi(m)}+1 \Longrightarrow 2p^{\alpha} \mid g^{\frac{1}{2}\varphi(m)}+1,$$

$$\therefore \quad \mathrm{imd}(-1) \equiv \frac{1}{2}\varphi(m)\ (\bmod \varphi(m))$$

(iii)若$m=4$，$\psi(4)=2$，则 m 有且只有一个原根 3，$\mathrm{ind}(-1)=\mathrm{ind}3\equiv 1=\frac{\psi(m)}{2}(\bmod m)$。

10. 若 a 是模m的平方剩余，则必存在整数 x，使得$x^2\equiv a$ $(\bmod m)$，$(a, m)=(x, a)=1\Longrightarrow x^{\varphi(m)}\equiv a^{\frac{1}{2}\varphi(m)}\equiv 1$ $(\bmod m)$，故 a 所属的方次数$\delta\leqslant\frac{1}{2}\varphi(m)$，所以 a 不可能是模 $m(\neq 2)$的原根，任何与 m 互素的整数，都是模m的平方剩余或平方非剩余，二者必居其一，所以模m的原根必是模m的平方非剩余。

11. 这个运算的规则是：在(a)中依次取其第 $1+2, 1+2\times 2$, $1+3\times 2$，…诸数后，剩下的部分（$\frac{n-1}{2}$项或$\frac{n}{2}$项）按倒序排列于后

面，而得到(a_1)〔或(a_1')〕；同法从(a_1)〔或(a_1')〕进行第二次运算，得到(a_2)〔或(a_2')等等。如，$n=9$，得

$$1,\ 3,\ 5,\ 7,\ 9,\ 8,\ 6,\ 4,\ 2; \qquad (a_1)$$

$$1,\ 5,\ 9,\ 6,\ 2,\ 4,\ 8,\ 7,\ 3; \qquad (a_2)$$

$$1,\ 9,\ 2,\ 8,\ 3,\ 7,\ 4,\ 6,\ 5; \qquad (a_3)$$

$$1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9. \qquad (a_4)$$

$k=4$，$1+2^4\equiv0\ (\mathrm{mod}17)$，即$2^4\equiv-1\ (\mathrm{mod}17)$。若$n=10$，则$k=9$时$(a)=(a_k)$。

实际上，从(a)到(a_k)运算的规律是：在序列

$$1,\ 2,\ \cdots,\ n-1,\ n,\ n,\ n-1,\ \cdots,\ 2;\ 1,\ 2,\ \cdots,\ n-1,\ n,\ n,\ n-1,\ \cdots,\ 2;\ \cdots;\ 1,\ 2,\ \cdots,\ n-1,\ n,\ n,\ n-1,\ \cdots,\ 2. \qquad (b)$$

中依次取出第1，$1+2^k$，$1+2\cdot2^k$，$1+3\cdot2^k$，$\cdots$，$1+(n-1)\cdot2^k$个位置上的数目排成一列，就得到$(a_k)=(a)$。这样的运算，也就是从(a)依题目所给的方法进行k次运算的结果.这种方法所进行的第k次运算。要求$1+2^k=2$。在(b)中除第二位是2 ($k=0$，0次运算，即序列(a)外，所有的2都在(b)的第$q(2n-1)$或$q(2n-1)+2$位的位置上出现，其中$q\geqslant1$。前者$2^k+1\equiv0\ (\mathrm{mod}2n-1)$，后者$2^k+1\equiv2\ \mathrm{mod}(2n-1)$。

$$\therefore\quad 2^k\equiv\pm1(\mathrm{mod}\ 2n-1).$$

这就证明了定理的必要性。

反之，若$2^k\equiv\pm1(\mathrm{mod}\ 2n-1)\Longrightarrow2^k+1\equiv0$或$2^k+1\equiv2(\mathrm{mod}\ 2n-1)$。序列$(a)$的第$k$次运算的结果，各位数字依次是$(b)$中第1，$1+2^k$，$1+2\cdot2^k$，$1+3\cdot2^k$，$\cdots$，$1+(n-1)2^k$个位置上的数目。

当$2^k+1=0(\mathrm{mod}\ 2n-1)$时，$(b)$的第$1+2^k$位是2，第$1+2\cdot2^k=2(1+2^k)-1$位是3，第$1+3\cdot2^k=3(1+2^k)-2$位是4，$\cdots$，$1+(n-1)2^k=(n-1)(1+2^k)-(n-2)$位是$n$。故经$k$次运算后仍得到$(a)$。

当$2^k-1\equiv0(\mathrm{mod}2n-1)$即$2^k+1\equiv2(\mathrm{mod}\ 2n-1)$，即$2^k+1=q(2n-1)+2$，取$q=1$，$(b)$中第$2^k+1=2n+1$位是2；第$1+2\cdot2^k$

$=2(2^k-1)+3$位是 3，…，$1+(n-1)2^k=(n-1)(2^k-1)+n$ 位是 n，故$(a_k)=(a)$。
这就证明了定理的充分性。

12． 仿前题，在(b)中除第二位外，所有 2 都在 $q(2n-1)$或 $q(2n-1)+2$ 的位置上($q\geqslant 1$前者$m^k+1\equiv 0(\bmod 2n-1)$，后者 $m^k+1\equiv 2(\bmod\ 2n-1)$。

$\therefore\quad m^k\equiv\pm 1(\bmod\ 2n-1)$。
这就证明了定理的必要性。

反之，若$m^k\equiv\pm 1(\bmod\ 2n-1)\Longrightarrow m^k+1\equiv 0$ 或 $m^k+1\equiv 2$ $(\bmod\ 2n-1)$。

序列(b)的第 k 次运算的前 n 位数字，依次是(b)的第 1，$1+m^k$，$1+2\cdot m^k$，$1+3m^k$，…，$1+(n-1)m^k$ 个位置上的数目。

当$m^k+1\equiv 0(\bmod 2n-1)$时，(b)的第 $1+m^k$位是 2，第 $1+2m^k=2(1+m^k)-1$ 位是 3，…，第 $1+(n-1)m^k=(n-1)(1+m^k)-(n-2)$位是n，故$(a_k)=(a)$。

当$m^k-1\equiv 0(\bmod 2n-1)$时，即 $m^k+1=q(2n-1)+2$，(b)中的这一位是 2，第 $2m^k+1=2q(m^k-1)+3$ 位是 3，第 $3m^k+1=3q(m^k-1)+4$ 位是 4，…，第 $(n-1)\cdot m^k+1=(n-1)q(m^k-1)+n$位 n。故经 k次运算后$(a^k)=(a)$。这就证明了充分性。

13． 由定理 6·9 知，$\varphi(m)=c=q_1^{\alpha_1}q_2^{\alpha_2}\cdots q_k^{\alpha_k}$时

$$g\in_m\varphi(m)\Longleftrightarrow g^{\frac{c}{g_i}}\not\equiv 1\ (\bmod m)$$

由欧拉定理，若$(x,\ m)=1$，则$x^c\equiv 1(\bmod m)$。

(i) 若 g 是模m的q_i次剩余，则$x^{q_i}\equiv g(\bmod m)$有解$\Longrightarrow 1\equiv x^c\equiv g^{\frac{c}{g_i}}(\bmod m)\Longrightarrow$ g 不是模m的原根。这就证明了必要性。

(ii) 反之，若 $x^{g_i}\equiv g(\bmod\ m)\ (i=1,\ \cdots,\ k)$ 无解，

则 g 是模m的原根。否则 $\exists g_t\ (1\leqslant t\leqslant k)\ni g^{\frac{c}{q_t}}\equiv 1\pmod m$，两边取指数得，$\frac{c}{q_t}\operatorname{ind}_{g'}g\equiv 0\pmod c\Longrightarrow \operatorname{ind}_{g'}g\equiv 0\pmod{q_t}$

$\Longrightarrow \operatorname{ind}_{g'}g=l_{q_t}$，由定义6·2得

$$g'^{l q_t}\equiv g\pmod m$$

所以 $x\equiv g'^{l}\pmod m$ 是 $x^{q_t}\equiv g\pmod m$ 的解。这与假设矛盾，这就证明了充分性。

14．(i) 因为 $\varphi(2^n+1)=2^n$，只有素因子 $q=2$，且 2^n、$1\ (n>1)$ 是素数，故 n 必为偶数，故由第13题知 3 是素数模 2^n+1 的一个原根。事实上，设 $n=2m$，则

$$\left(\frac{3}{2^n+1}\right)=\left(\frac{2^n+1}{3}\right)=\left(\frac{(2^2)^m+1}{3}\right)=\left(\frac{2}{3}\right)=-1,$$

即 3 是模 2^n+1 的平方非剩余。

(ii) 因为 $\varphi(2p+1)=2p$，它的素因子有且只有 $q_1=2, q_2=p$。当 $p=4n+1$ 时，

$$\left(\frac{2}{2p+1}\right)=(-1)^{\frac{(2p+1)^2-1}{8}}=(-1)^{\frac{1}{2}p(p+1)}$$

$$=(-1)^{(4n+1)(2n+1)}=-1,$$

且 $x^p\equiv 2\pmod{2p+1}$ 无解。否则，因 $(x,2p+1)=(2,2p+1)=1$，故 $x^{2p}\equiv 2^2\not\equiv 1\pmod{2p+1}$ 与 $x^{2p}\equiv 1\pmod{2p+1}$ 矛盾。

当 $n=4n+3$ 时，

$$\left(\frac{-2}{2p+1}\right)=\left(\frac{-1}{2p+1}\right)\left(\frac{2}{2p+1}\right)=$$

$$=(-1)^p(-1)^{\frac{1}{2}p(p+1)}=$$

$$=(-1)^{4n+3}(-1)^{2(n+1)(4n+3)}=-1,$$

且 $x^p \equiv -2 \pmod{8n+7}$ 无解。否则 $4 \equiv 1 \pmod{8n+7}$ 这就不可能的。

综上所述，故 2 是形如 $8n+3$ 的素数的原根，-2是形如$8n+7$的素数的原根。

(iii) 因为$\varphi(4p+1)=4p$，p 是奇素数，故

$$\left(\frac{2}{4p+1}\right)=(-1)^{p(2p+1)}=-1,$$

且 $x^p \equiv 2 \pmod{4p+1}$ 无解，否则，$2^4 \equiv 1 \pmod{4p+1}$，而 $4p+1$是不等于3，5 的素数，故$16 \not\equiv 1 \pmod{4p+1}$，矛盾。所以 2 是模形如$4p+1$素数的原根。

(iv) 因为 $\varphi(2^n p+1)=2^n p\ (n>1)$ 有且只有素因子 2 和 p，而

$$\left(\frac{3}{2^n p+1}\right)=\left(\frac{2^n p+1}{3}\right)=\left(\frac{2}{3}\right)=-1,$$

且对任一整数 x，$x^p \not\equiv 3 \pmod{2^n p+1}$。否则，

$$3^{2^n} \equiv 1 \pmod{2^n p+1},\ n^2>1,\ p>\frac{3^{2^{n-1}}}{2^n} \Longrightarrow (3^{2^{n-1}}+1)$$

$$(3^{2^{n-1}}-1) \equiv 0 \pmod{2^n p+1} \Longrightarrow (2^n p+1) \mid (3^{2^{n-1}}+1) \text{或}$$

$$(2^n p+1) \mid (3^{2^{n-1}}-1).$$

而$2^n p+1>3^{2^{n-1}}+1$ 故这是不可能的。所以 3 是模$2^n p+1$的原根。

15. $\varphi(17)=16$，它有且只有素因子 2。而

$$\left(\frac{10}{17}\right)=\left(\frac{2}{17}\right)\left(\frac{5}{17}\right)=(-1)^{36}\left(\frac{17}{5}\right)=\left(\frac{2}{5}\right)=-1,$$

由第13题知，10是模17的原根。

$\varphi(257)=256=2^8$，有且只有素因子 2，而

$$\left(\frac{10}{257}\right)=\left(\frac{2}{257}\right)\left(\frac{5}{257}\right)=\left(\frac{257}{5}\right)=\left(\frac{2}{5}\right)=-1,$$

所以10是模257原根。

由定理6·2的系2的证明过程中知 $\frac{1}{17}$，$\frac{1}{257}$ 循环节的长度t，是使

$10^t\equiv 1(\mathrm{mod}\,17)$，$10^t\equiv 1(\mathrm{mod}\,257)$

成立的最小整数，因为10是模17，257的原根，所以 $t=16$，256。

16. $c=\varphi(83)=82$，$(2,82)=2$，$\mathrm{ind}\,59=20$，$2|20$，由定理6·14知原同余式有二解。且 $x^2\equiv 59(\mathrm{mod}\,83)$ 等价于

$2\,\mathrm{ind}\,x\equiv \mathrm{ind}\,59(\mathrm{mod}\,82)\Longrightarrow \mathrm{ind}\,x\equiv 10(\mathrm{mod}\,41)\Longrightarrow \mathrm{ind}\,x\equiv 10,\ 51(\mathrm{mod}\,82)\Longrightarrow x\equiv \pm 15(\mathrm{mod}\,83)$。

(ii) $\varphi(43)=42$，$(2,42)=2$，$\mathrm{ind}\,32=27$，$2\nmid 27$，故原同余式无解。

(iii) $\varphi(53)=52$，$(2,52)=2$，$\mathrm{ind}(-17)=\mathrm{ind}\,36=16$，$2|16$，有二解。与(i)同样的计算，可得 $x\equiv\pm 6(\mathrm{mod}\,53)$ 是原同余式的解。

(iv) $\varphi(89)=88$，$18x\equiv 42(\mathrm{mod}\,89)$ 即 $3x\equiv 7(\mathrm{mod}\,89)\Longrightarrow \mathrm{ind}\,3+\mathrm{ind}\,x\equiv \mathrm{ind}\,7(\mathrm{mod}\,88)\Longrightarrow \mathrm{ind}\,x\equiv 7-87\equiv 8(\mathrm{mod}\,88)\Longrightarrow x\equiv 32(\mathrm{mod}\,89)$。

(v) 与上题同法可解得 $x\equiv 55(\mathrm{mod}\,97)$。

(vi) $\varphi(41)=40$，$(40,3)=1$，有唯一解。与(i)一样地，解得 $x\equiv 7(\mathrm{mod}\,41)$。

(vii) $\varphi(29)=28$，$(5,28)=1$，有唯一解。解得 $x\equiv 17(\mathrm{mod}\,29)$。

(viii) $\varphi(61)=60$，$(60,7)=1$，有唯一解。解得 $x\equiv 27(\mathrm{mod}\,61)$。

(ix) $\varphi(43)=42$，$(3,42)=3$，$\mathrm{ind}\,22=3$，$3|\mathrm{ind}\,22$，故有三个解。

$x^3\equiv 22(\mathrm{mod}\,43)\Longrightarrow 3\,\mathrm{ind}\,x\equiv 3(\mathrm{mod}\,42)\Longrightarrow \mathrm{ind}\,x\equiv 1(\mathrm{mod}\,14)\Longrightarrow \mathrm{ind}\,x\equiv 1,\ 15,\ 29(\mathrm{mod}\,42)\Longrightarrow x\equiv 28,\ 39,\ 19(\mathrm{mod}\,43)$。

(x) $\varphi(53)=52$；$(6,52)=2$，$\mathrm{ind}\,15=40$，$2|=40$，故有二

解。解得$x\equiv\pm4 \pmod{53}$。

(xi) $\varphi(59)=58$，$(58,4)=2$，ind 11 = 45，$2\nmid45$，故无解。

(xii) $5x\equiv13 \pmod{3^3}$，由于$(5,27)=1$故原同余式有且只有一个解。先求$2x\equiv1 \pmod 3$的解$x\equiv2 \pmod 3$。次解

$5(2+3t_1)-13\equiv0 \pmod 9 \Longrightarrow t_1\equiv2, 5, 8 \pmod 9 \Longrightarrow$ 取$t_1=2$，得$x\equiv8 \pmod 9$是$5x\equiv13 \pmod 9$的解

$5[2+3(2+3t_2)]13\equiv \pmod{27} \Longrightarrow t_2\equiv0 \pmod{27} \Longrightarrow x\equiv8 \pmod{27}$ 是原同余式的解。

(xiii) 先求$x^2\equiv1 \pmod 3$的解$x\equiv\pm1 \pmod 3$，次求$(1+3t_1)^2\equiv1 \pmod 9$的解

$(1+3t_1)^2\equiv1 \pmod 9 \Longrightarrow t_1(3t_1+2)\equiv0 \pmod 3 \Longrightarrow$

$t_1\equiv0, 3, 6 \pmod 9 \Longrightarrow x_1\equiv\pm1, \pm10, \pm19 \pmod 9$是$x^2\equiv10 \pmod 9$的解。由于原同余式有且只有两解，可从$x\equiv\pm1 \pmod 3$导出。仿(xii)方法解得$x\equiv\pm8 \pmod{27}$是原同余式的解。

第七章

1. 若$\xi=[1, 10, 10^{2!}, \cdots, 10^{(n-1)!}, \cdots]=[a_1, a_2, a_3, \cdots, a_n, \cdots]$，由定理1·6的系知道：$\xi$的第 n 个渐近分数$\frac{P_n}{Q_n}$满足

$$\left|\xi-\frac{P_n}{Q_n}\right|<\frac{1}{Q_nQ_{n+1}}=\frac{1}{Q_n(a_{n+1}Q_n+Q_{n-1})}<\frac{1}{a_{n+1}Q_n^2}$$

$$\because\quad Q_n=a_nQ_{n-1}+Q_{n-2}>a_nQ_{n-1}>a_na_{n-1}Q_{n-2}>\cdots>a_n\cdots a_1$$
$$=10^{(n-1)!+(n-2)!+\cdots+2!+1}$$

$$a_{n+1}Q^2>10^{n!+2[(n-1)!+\cdots+2+1]}>a_n^{n+2}>a_n^n$$

$$\therefore\quad \left|\xi-\frac{P_n}{Q_n}\right|<\frac{1}{a_n^n}$$

$$\because\quad Q_n=a_nQ_{n-1}+Q_{n-2}<(a_n+1)Q_{n-1}<$$
$$<(a_n+1)(a_{n-1}+1)Q_{n-2}<\cdots<$$

$$<(a_n+1)\cdots(a_3+1)(a_2+1)$$

$$=(10^{(n-1)!}+1)\cdots(10^{2!}+1)(10+1)<$$

$$<10^{[(n-1)!+1]+\cdots+[2!+1]+[1+1]}$$

$$=10^{(n-1)+[1+2!+\cdots+(n-1)!]}<10^{2\cdot(n-1)!}$$

$$=a_n^2\quad(n\geqslant5)$$

事实上，A) $n=5$，$2\cdot(n-1)!=48$，$(n-1)+[1+2!+3!+4!]=37$，故 $2(5-1)!>(5-1)+(1+2!+3!+4!)$。$n=6$时，$2\times5!=240$，$5+[1+\cdots+5!]=156$，因 $240>156$。故 $n=6$ 时，$2\cdot(n-1)!>(n-1)[1+2!+\cdots+(n-1)!]$。

B) 若小于 k 时不等式成立，则

$$2\cdot(k-1)!=2(k-1)\cdot(k-2)!>(k-1)[(k-2)+(1+2!+\cdots+(k-2)!]=(k-1)(k-2)+[(k-1)+2!(k-1)+\cdots+(k-1)(k-3)!+(k-1)!]<(k-1)+[1+2!+\cdots+(k-2)!+(k-1)!],\ (k\geqslant5)$$

$$\therefore\quad a_n^2>Q_n,\ (n\geqslant5)$$

于是

$$\left|\xi-\frac{P_n}{Q_n}\right|<\frac{1}{a_n^n}<\frac{1}{Q_n^{\left[\frac{1}{2}n\right]}}<\frac{1}{Q_n^{\left[\frac{1}{2}N\right]}}$$

对于 $\forall n>N$ 上不等式都成立，这样的 n 有无限多，故由定理7·6的逆否定理，知 ξ 是超越数。

2. 若 α 是一个首项系数 $a_n\geqslant1$ 的整系数多项式的根，则

$$a_n\alpha^n+a_{n-1}\alpha^{n-1}+\cdots+a_1\alpha+a_0=0\Longrightarrow(a_n\alpha)^n+a_{n-1}(a_n\alpha)^{n-1}+\cdots+a_1a_n^{n-2}(a_n\alpha)+a_0a_n^{n-1}=0$$

所以令 $q=a_n$，则 $q\alpha$ 是代数整数。

3. 若 $a_n\theta^n+a_{n-1}\theta^{n-1}+\cdots+a_1\theta+a_0=0$，则

$$a_0\left(\frac{1}{\theta}\right)^n+a_1\left(\frac{1}{\theta}\right)^{n-1}+\cdots+a_{n-1}\left(\frac{1}{\theta}\right)+a_n=0.$$

因 $\theta^{-1}=\left(\frac{1}{\theta}\right)$，且$a_n=1$，$a_0=\pm1$，故 θ 与 θ^{-1}都是代数整数，且 $\theta\theta^{-1}=1$，即 θ 是 $k(\xi)$的单位。反之，若 θ 是 $k(\xi)$ 的单位，则 θ 和 θ^{-1}都满足一个首项系数为 1 的整系数多项式，并且它们是：

$$a_n\theta^n+a_{n-1}\theta^{n-1}+\cdots+a_1\theta+a_0=0$$

$$a_0(\theta^{-1})^n+a_1(\theta^{-1})^{n-1}+\cdots+a_{n-1}\theta^{-1}+a_n=0\ .$$

故 $a_n=1$，$a_0=\pm1$。

4．因为 $\xi=a+bi$ 是 $x^2-2ax+a^2+b^2$ 的根，故 ξ 是二次整数（自然 $b=0$时它是一次整数）。

$\xi\pm\eta=(a\pm c)+(b\pm d)i=e+fi$，$e$，$f\in R$，故它们也是二次整数，即 $\xi+\eta\in R[i]$。$\xi\eta=ac-bd+(ad+bc)i\in R[i]$，所以$R[i]$是一个数环。

若 α，β，…，$\gamma\in R[i]$，则它们以及$R[i]$的数经有限次加、减、乘运算的结果仍属于$R[i]$，故 $\xi=f(\alpha,\beta,\cdots,\gamma)\in R[i]$，$\xi$ 是一个二次整数。

5．1° 因为 $\rho^2+\rho+1=0$，故 ρ 是二次整数。

2° $a+b\rho=a+b\left(-\frac{1}{2}+\frac{1}{2}i\sqrt{3}\right)=a-b-b\left(-\frac{1}{2}-\frac{1}{2}i\sqrt{3}\right)=a-b-b\rho^2\left(\because\ \rho^2=-\frac{1}{2}-\frac{1}{2}i\sqrt{3}\right)$.

$a+b\rho^2=a+b\left(-\frac{1}{2}-\frac{1}{2}i\sqrt{3}\right)=a-b-b\left(-\frac{1}{2}+\frac{1}{2}i\sqrt{3}\right)$
$=a-b-b\rho$.

3° 因为 $-3\equiv1(\mathrm{mod}\ 4)$，故$R[\sqrt{-3}]$的任一元素是 $a-\frac{b}{2}+\frac{b}{2}\sqrt{-3}=a+b\rho$，

$$\therefore\qquad R[-\sqrt{-3}]=R[\rho]$$

4° $\because$ $N(\xi)=\left[\left(a-\frac{b}{2}\right)+\frac{b}{2}\sqrt{-3}\right]\left[\left(a-\frac{b}{2}\right)-\right.$

$$-\frac{b}{2}\sqrt{-3}\,]\Big|$$

$$=|a^2-ab+b^2|$$

$$=a^2-ab+b^2$$

又因 $\rho^2+\rho=-1$，$\rho^3=1$，故

$$|(a+b\rho)(a+b\rho)^2|=|a^2-ab+b^2|=a^2-ab+b^2$$

因而结论成立。

5° 要求 $N(\xi)=\pm1$，即要求

$$a^2-ab+b=1\Longrightarrow(2a-b)^2+3b^2=4$$

的一切整数解。故有且只有 $a=\pm1$，$b=0$；$b=\pm1$，$a=0$；$a=1$，$b=1$；$a=-1$，$b=-1$。即 ±1，$\pm\rho$，$\mp\rho^2$ 是R[ρ]的单位，并且再无其他单位了。

6° $$\frac{\alpha}{\beta}=\frac{a+b\rho}{c+d\rho}$$

$$=\frac{(a+b\rho)(c+d\rho^2)}{(c+d\rho)(c+d\rho^2)}$$

$$=\frac{(ac+bd-ad)+(bc-ad)\rho}{c^2-cd+d^2}$$

$$=S+T\rho$$

其中 S，T∈K，存在二有理整数 x 和 y，使得

$$|S-x|\leqslant\frac{1}{2},\quad|T-y|\leqslant\frac{1}{2}$$

令 $\delta=x+y\rho$，则

$$\left|\frac{\alpha}{\beta}-\delta\right|^2=|(S-x)+(T-y)\rho|^2$$

$$=(S-x)^2-(S-x)(T-y)+(T-y)^2\leqslant\frac{3}{4}$$

因为 α，β，δ∈R[ρ]，故取 $\gamma=\alpha-\delta\beta\in R[\rho]$，且

$$N(\gamma)=N(\alpha-\delta\beta)\leqslant\frac{3}{4}N(\beta)<N(\beta)$$

$$\therefore\quad\alpha=\beta\delta+\gamma,\quad N(\gamma)<N(\beta)$$

7° 因为 $N(1-\rho)=3$ 是有理素数，故 $1-\rho$ 是素数。事实上，若

$1-\rho=(a+b\rho)(c+d\rho)$，则$3=N(a+b\rho)$。$N(c+d\rho)\Longrightarrow$
$\Longrightarrow N(a+b\rho)=1$或$N(c+d\rho)=1$。

$\because\ \lambda^2=1-2\rho+\rho^2=-3\rho$

而$-\rho$是单位，故 3 与 λ^2 相伴。

8° 若 $p\equiv1(\mathrm{mod}\ 3)$，$p=3n+1$为素数时，只能 (i) $n=4m+2$，

则 $\left(\frac{-3}{p}\right)=(-1)^{\frac{12m+6}{2}}\left(\frac{3}{12m+7}\right)=(-1)(-1)\left(\frac{1}{3}\right)=1$；

(ii) $n=4m$，则 $\left(\frac{-3}{p}\right)=(-1)^{\frac{12m}{2}}\left(\frac{3}{12m+1}\right)=1$。

$\therefore\ \left(\frac{-3}{p}\right)=1\Longrightarrow p\mid x^2+3\Longrightarrow x^2+3=(x-\sqrt{-3})(x+\sqrt{-3})=$
$=kp$，若 p 是$R[\rho]$中的素数，则 $p\mid x-\sqrt{-3}$，或 $p\mid x+\sqrt{-3}$ 是不可能的。故 p 不是素数。因而

$p=(a+b\rho)(a+b\rho^2)=a^2-ab+b^2$

9° 从7° 和8°已知(i)(iii)正确。令证$3n+2=p$是$R[\rho]$的素数。$2=a^2-ab+b^2$无整数解，故 2 是素数。一般地，$p=3n+2=a^2-ab+b^2$无整数解。事实上，由于$(3t+1)^2\equiv1(\mathrm{mod}\ 3)$，$(3t-1)^2\equiv1(\mathrm{mod}\ 3)$，$(3t)^2\equiv0(\mathrm{mod}\ 3)\Longrightarrow$(i) 若$a=3t+1$，$b=3s+1\Longrightarrow a^2+b^2-ab=3k+1$或$3k$；(ii)$a=3t+1$，$b=3s\Longrightarrow a^2+b^2-ab=3k+1$；(iii) $a=3t$，$b=3s\Longrightarrow a^2+b^2-ab=3k$。

所以 $p=3n+2$ 是 $R[\sqrt{-3}]$的素数。

10° 任给$\gamma\in R[\rho]$，我们有

$\gamma=a+b\rho=a+b-b\lambda\equiv a+b(\mathrm{mod}\ \lambda)$

因为$3=(1-\rho)(1-\rho^2)\Longrightarrow\lambda\mid3$，而 $a+b$ 关于模 3 仅同余于 -1，0，1 之一。故结论正确。

6. 用反证法，若$m\sqrt{N}=\frac{a}{b}$，a，$b\in R$，$(a,b)=1$，则$a^m=b^mN$，又因$N>1$，故 $a>1$，由于$(a,b)=1\Longrightarrow(a^m,b^m)=1$
$\Longrightarrow a^m\mid N$，与假设矛盾。

7　若$x_0=\frac{a}{b}$，$(a,\ b)=1$是(1)的有理根，则

$$\left(\frac{a}{b}\right)^m+c_1\left(\frac{a}{b}\right)^{m-1}+\cdots+c_{m-1}\left(\frac{a}{b}\right)+c_m=0$$

$$\Longrightarrow a^m+c_1a^{m-1}b+\cdots+c_{m-1}ab^{m-1}+c_mb^m=0$$

$$\Longrightarrow a(a^{m-1}+c_1a^{m-2}b+\cdots+c_{m-1}b^{m-1})=-c_mb^m,$$

或者 $a^m=-b(c_1a^{m-1}+\cdots+c_{m-1}ab^{m-2}+C_mb^{m-1})$

$$\Longrightarrow a|c_m \text{ 且 } b|1$$

$$\Longrightarrow b=1$$

$$\Longrightarrow x_0=a$$

所以(1)的有理根必为整根，因此除整根之外的实根必为无理根．

8　因为$\sqrt{2}+\sqrt{3}$是无有理根的方程

$$x^4-10x+1=0 \tag{a}$$

的根，由第7题知道$\sqrt{2}+\sqrt{3}$是(a)的无理根，故$\sqrt{2}+\sqrt{3}$是无理数。

9。若$\lg 2=\frac{a}{b}$，$a,\ b\in R$，$(a,\ b)=1\Longrightarrow 10^{\frac{a}{b}}=2\Longrightarrow 10^a=$

$=2^b\Longrightarrow 2^a5^a=2^b\Longrightarrow 5^a=2^{b-a}$　　$(a\neq 0)$

这是不可能的，故 lg 2是无理数。

同理，若$\log_n m=\frac{a}{b}\Longrightarrow n^a=m^b$。

因为$m\neq n^t(t=0,\ \pm 1,\ \pm 2,\ \cdots)$，若$(m,\ n)=d<n$，$m=dm_1$，$n=dn_1(n_1>1)$，$(m_1,\ n_1)=1$，则

$$n^a=m^b\Longrightarrow n_1^a=m_1^b d^{b-a}\ (b>0)\Longrightarrow m_1^b\ \Big|\ n_1^a$$

这是不可能的。所以$\log_n m$是无理数。

10。若$y=\frac{k}{h}$且e^y是有理数，则$e^{hy}=e^k$是有理数，这是不可能的。否则，$e^k=\frac{a}{b}$，这里a，b都是正整数。我们写

$$F(x)=k^{2n}f(x)-k^{2n-1}f'(x)+\cdots-hf^{(2n-1)}(x)+f^{(2n)}(x)$$

其中 $f(x)=\dfrac{x^n(1-x)^n}{n!}=\dfrac{1}{n!}\sum\limits_{m=n}^{2n}c_m x^m$，$c_m\in R$。因而$F(0)$和$F(1)$都是有理整数。我们有

$$\frac{d}{dx}\{e^{kx}F(x)\}=e^{kx}\{kF(x)+F'(x)\}=k^{2n+1}e^{kx}f(x)$$

因而

$$b\int_0^1 k^{2n+1}e^{kx}f(x)dx=b[e^{kx}F(x)]_0^1=aF(1)-bF(0)$$

是一个整数。

由于当$0<x<1$时，$0<f(x)<\dfrac{1}{n!}$，所以当 n 足够大时，有

$$0<b\int_0^1 k^{2n+1}e^{kx}f(x)dx<\frac{bk^{2n}e^k}{n!}<1,$$

矛盾。

11. 若 $\pi^2=\dfrac{a}{b}$ 是有理数 $a>0$，$b>0$是整数，

令

$$G(x)=b^n\{\pi^{2n}f(x)-\pi^{2n-2}f''(x)+\pi^{2n-4}f^{(4)}(x)-\cdots+(-1)^n f^{(2n)}(x)\}$$

其中$f(x)=\dfrac{x^n(1-x)^n}{n!}$，因此$G(0)$和$G(1)$都是整数。我们有

$$\frac{d}{dx}\{G'(x)\sin\pi x-\pi G(x)\cos\pi x\}$$

$$=\{G''(x)+\pi^2G(x)\}\cdot\sin\pi x=b^n\pi^{2n+2}f(x)\sin\pi x=$$

$$=\pi^2a^n\sin\pi x f(x)$$

$$\therefore\quad \pi^2\int_0^1 a^n\sin\pi x f(x)dx=[G'(x)\sin\pi x/\pi-G(x)\cos\pi x]_0^1$$

$$=G(0)+G(1)$$

是一个整数。但是由于当$0<x<1$时，$0<f(x)<\dfrac{1}{n!}$，因而对充分大的 n 有

$$0<\pi^2\int_0^1 a^n\sin\pi x f(x)dx<\frac{\pi a^n}{n!}<1,$$

矛盾。

12. $\because\ \sin 1 = 1 - \frac{1}{3!} + \frac{1}{5!} - \cdots + (-1)^n \frac{1}{(2n-1)!} +$

$$+ (-1)^{n+1} \frac{1}{(2n+3)!}\left[1 - \frac{(2n+3)!}{(2n+5)!} + \cdots\right]$$

显然，$0 < 1 - \frac{(2n+3)!}{(2n+5)!} + \cdots < 1$。若$\sin 1 = \frac{a}{b}$，$(a, b) = 1$，选取奇数 n 使$2n+3 > b$，则

$$(2n+3)!\frac{a}{b} = (2n+3)!\left[1 - \frac{1}{3!} + \cdots + (-1)^n \frac{1}{(2n+1)!}\right] +$$

$$+ (-1)^{n+1}\left[1 - \frac{(2n+3)!}{(2n+5)!} + \cdots\right] = I + \alpha$$

上式左边是整数，右边前一项I是整数，后一项$0 < |\alpha| < 1$，这是不可能的。故 sin 1是无理数。

13. 若$\log_3 2$ 是有理数$\Longrightarrow \log_3 2 = \frac{p}{q}$，$(p, q) = 1$，$p > 0$，$q > 0 \Longrightarrow 3^{\frac{p}{q}} = 2 \Longrightarrow 3^p = 2^q \Longrightarrow 3 | 2^q \Longrightarrow 3 | 2$，这是不可能的，故$\log_3 2$是无理数。

令 $\ln 3 = x$，$\ln 2 = y \Longrightarrow e^x = 3$，$e^y = 2 \Longrightarrow x\log_3 e = 1$，$y\log_3 e = \log_3 2 \Longrightarrow \frac{\ln 3}{\ln 2} = \frac{1}{\log_3 2}$是无理数。

14. 若$\frac{\ln 3}{\ln 2}$不是超越数，由13题知，$\frac{\ln 3}{\ln 2}$是非有理数的代数数。由13题证明过程中知道$3 = 2^{\frac{\ln 3}{\ln 2}}$是超越数$\Longrightarrow$3是超越数。矛盾。

15. 设M是素数，则

$$M \equiv 8 \cdot 16^n - 1 \equiv 8 - 1 \equiv 2 \pmod 5$$

在(30)中取$\alpha = \omega$，$q = M$，，得

$$\bar{\omega} \equiv \omega^{M+1} = \omega^{2^p} \equiv \omega\bar{\omega} = -1 \pmod M \Longrightarrow \gamma_{p-1} =$$

$$= \omega^{2^{p-1}}(\omega^{2^p} + 1) \equiv 0 \pmod M$$

故(1)成立。

这个条件还是充分的，充分性这里不证。

第八章

1。因为 $\sigma(n)\geqslant 2n$，两边同乘m，得

$$m\sigma(n)\geqslant 2mn$$

又由于 m 与 n 的每一个因数之积，都是mn 的因数，所以

$$\sigma(mn)\geqslant m\sigma(n)\geqslant 2mn$$

又因 $m\geqslant 2$，故 $m\sigma(n)$不包含 mn 的因子 1，于是

$$\sigma(mn)>m\sigma(n)\geqslant 2mn$$

2。若 n是亏数，而 $d|n$的 d 是完全数或盈数，则由上题知，$\frac{n}{d}\times d=n$ 是盈数，矛盾．

3。$\because \sigma(p^n)=1+p+\cdots+p^{n-1}+p^n$

$$=\frac{p^n-1}{p-1}+p^n<2p^n$$

所以 p^n 是亏数。

4。若 $n=m^2=2^{2\alpha}p_1^{2\alpha_1}p_2^{2\alpha_2}\cdots p_k^{2\alpha_k}$，则

$\sigma(n)=\sigma(m^2)$

$$=(1+2+\cdots+2^{2\alpha})(1+p_1+\cdots+p_1^{2\alpha_1})(1+p_2+\cdots p_2^{2\alpha_2})\cdots$$

$$(1+p_k+\cdots+p_k^{2\alpha_k})$$

上式右边各因子都是奇数，故 $\sigma(n)$是奇数。

若 $n=2m^2=2^{2\alpha+1}p_1^{2\alpha_1}\cdots p_k^{2\alpha_k}(\alpha\geqslant 0,\alpha_i>0,\ i=1,\ \cdots,\ k)$，则

$\sigma(n)=\sigma(2m^2)$

$$=(1+2+\cdots+2^{2\alpha+1})(1+p_1+\cdots+p_1^{2\alpha_1})\cdots$$

$$\cdots(1+p_k+\cdots+p_k^{2\alpha_k})$$

上式右边各因子都是奇数，故 $\sigma(n)$是奇数。

反之，若 $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$，且 $\sigma(n)$为奇数，则

$$\sigma(n)=(1+p_1+\cdots+p_1^{\alpha_1})(1+p_2+\cdots+p_2^{\alpha_2})\cdots$$
$$\cdots(1+p_k+\cdots+p_k^{\alpha_k})$$

仅当右边各因子都是奇数，即 α_1，α_2，…，α_k 都是偶数时，或当 $p_1=2$时允许 α_1是奇数，α_2，…，α_k 都是偶数时，$\sigma(n)$为奇数，故 $n=m^2$或$2m^2$。

5. 因为 n 是奇数，若$\sigma(n)=2n$，则$2\,/\!\!/\,2n$。且 n 只有奇素数的因数，若$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$，$\sigma(n)=(1+p_1+\cdots+p_1^{\alpha_1})(1+p_2+\cdots+p_2^{\alpha_2})\cdots(1+p_k+\cdots+p_k^{\alpha_k})$的右边的 k 个因子中只能有一个是2的奇数倍，其他 $k-1$个因子都是奇数，可设 $p_1=p$，$\alpha_1=2\alpha'+1$ α_2，…，α_k 都是偶数，即$p_2^{\alpha_2}\cdots p_k^{\alpha_k}=q^2$。但是

$$1+p+\cdots+p^{2\alpha'+1}=\frac{p^{2\alpha'+2}-1}{p-1}$$
$$=\frac{p^{\alpha'+1}-1}{p-1}(p^{\alpha'+1}+1)$$
$$=(1+p+\cdots+p^{\alpha'})\times 2k$$

要求$1+p+\cdots+p^{\alpha'}$是奇数，必须$\alpha'=2\alpha$为偶数。所以$\sigma(n)=2n$的必要条件是 $n=p^{4\alpha+1}q^2$。

6.（1） 由于除 2，3 二素数之外，一切素数都是形如 $6n+1$或$6n-1$形，且两个$6n+1$形的素数之积仍是$6n+1$形。令

$$q=2\cdot3\cdot5\cdots p-1=6m-1$$

必有一个素数 $p'>p$，使$p'|q\Longrightarrow q=p'k$。若$p'$是$6n-1$形则结论成立，否则 k 必为 $6n-1$形，它存在一个大于 p 的素因子 p''，若 p''

是6n－1形，则结论成立，否则可依此类推，知道总存在一个大于p的6n－1形的素数。由于 p 的任意性，故6n－1形的素数数目是无穷的。

（2） 取 q 表示如下的两个互素的数的的平方和：

$$q=3^2\cdot5^2\cdot7^2\cdots p^2+2^2$$

由于任一奇数2m＋1的平方

$$(2m+1)^2=4m(m+1)+1\equiv1\pmod 8$$

$$\therefore\qquad q\equiv5\pmod 8$$

由于两个8n＋1形的数之积仍为 8n＋1形，如用（1）的方法，知道q必有一个大于 p 的8n＋5形的素因子，故结论成立。

7. 取$[\xi]=b$，则

$$\int_a^b f(x)dx=\sum_{i=a}^{b-1}\int_i^{i+1} f(x)dx\begin{cases}\geqslant\sum\limits_{i=a}^{b-1} f(i)\\ \leqslant\sum\limits_{i=a}^{b-1} f(i+1)\end{cases}$$

即

$$f(a)+\cdots+f(b-1)\leqslant\int_a^b f(x)dx\leqslant f(a+1)+\cdots+f(b);$$

又

$$0\leqslant\int_b^\xi f(x)dx\leqslant f(\xi)$$

$$\therefore\qquad\left|\sum_{a\leqslant n\leqslant\xi} f(n)-\int_a^\xi f(x)dx\right|\leqslant f(\xi)$$

8. 令$f(x)=\ln x$，$T(\xi)=\sum\limits_{n\leqslant\xi}\ln n$，从上题的不等式，得

$$\left|T(\xi)-\int_1^\xi\ln x\,dx\right|\leqslant\ln\xi\Longrightarrow\left|T(\xi)-\xi\ln\xi+\xi-1\right|\leqslant\ln\xi.$$

特别当ξ为整数n时，则

$$n\ln n-n+1-\ln n\leqslant\ln n!\leqslant n\ln n-n+1+\ln n$$

$$\therefore\qquad n^{n-1}e^{-n+1}\leqslant n!\leqslant n^{n+1}e^{-n+1}$$

事实上，$n\ln n-n+1-\ln n=\ln(n^{n-1}e^{-n+1})$，
$n\ln n-n+1+\ln n=\ln(n^{n+1}e^{-n+1})$。

9. (i) 把(1)关于变数 s 逐项求微商，即得(2)。

(ii) 设 $p\geqslant 2$，对 $s>1$(实际上 $s>0$即可)

有

$$\frac{1}{1-p^{-s}}=1+p^{-s}+p^{-2s}+\cdots$$

若取 $p=2, 3, \cdots, P$，则右边乘积的一般项

$$2^{-a_2s}3^{-a_3s}\cdots P^{-a_Ps}=n^{-s}$$

这里 $n=2^{a_2}3^{a_3}\cdots P^{a_P}(a_2\geqslant 0, a_3\geqslant 0, \cdots, a_P\geqslant 0)$，n无大于 P 的素因子。当没有大于P的素因子之积的数都可表成n形，所以

$$\prod_{p\leqslant P}\frac{1}{1-p^{-s}}=\sum_{(P)}n^{-s}$$

右边的和式的n是过一切不大于P而伸展到P的素数之幂之积。这些数包括一切素因子不大于P的数，因而

$$0<\sum_{n=1}^{\infty}n^{-s}-\sum_{(P)}n^{-s}<\sum_{P+1}^{\infty}n^{-s}$$

最后一个和式，当$P\to\infty$时趋向于0。所以

$$\zeta(s)=\sum_{n=1}^{\infty}n^{-s}=\lim_{P\to\infty}\sum_{(P)}n^{-s}=\lim_{P\to\infty}\prod_{p\leqslant P}\frac{1}{1-p^{-s}}$$

(iii) $\zeta(s)$可写成如下的形式

$$\zeta(s)=\sum_{n=1}^{\infty}n^{-s}=\int_1^{\infty}x^{-s}dx+\sum_{n=1}^{\infty}\int_n^{n+1}(n^{-s}-x^{-s})dx \qquad (\alpha)$$

这里 $\int_1^{\infty}x^{-s}dx=\frac{1}{s-1}$ ($\because s>1$)亦即

$$0<n^{-s}-x^{-s}=\int_n^x st^{-s-1}dt<\frac{s}{n^s}\ (n<x<n+1)$$

$$\therefore \qquad 0<\int_n^{n+1}(n^{-s}-x^{-s})dx<\frac{s}{n^2}$$

并且 $0<\sum_{n=1}^{\infty}\int_n^{n+1}(n^{-s}-x^{-s})dx<s\sum_{n=1}^{\infty}n^{-2}$.

$$\therefore \quad \zeta(s)=\frac{1}{s-1}+O(1) \tag{4}$$

(iv) 由(4)得

$$\ln\zeta(s)=\ln\frac{1}{s-1}+\ln\{1+O(s-1)\}$$

$$\therefore \qquad \ln\zeta(s)=\ln\frac{1}{s-1}+O(s-1)$$

(v) $$-\zeta'(s)=\sum_{n=1}^{\infty}n^{-s}\ln n=\int_1^{\infty}x^{-s}\ln x dx$$

$$+\sum_{n=1}^{\infty}\int_n^{n+1}(n^{-s}\ln n-x^{-s}\ln x)dx=$$

$$=\left[x^{-s+1}\left(\frac{\ln x}{-s+1}-\frac{1}{(s-1)^2}\right)\right]_1^{\infty}+$$

$$+\left[n^{-s}\ln n\cdot x-x^{-s+1}\left(\left(\frac{\ln x}{-s+1}\right)-\right.\right.$$

$$\left.\left.-\frac{1}{(s-1)^2}\right)\right]_n^{n+1}=\frac{1}{(s-1)^2}+k_1$$

$$\therefore \quad \zeta'(s)=-\frac{1}{(s-1)^2}+O(1)$$

第九章

1. 由定理9·5的证明(ii)中知道，当$d=-36<0$，$a>0$时，必有$a\leqslant\sqrt{\frac{|d|}{3}}=\sqrt{12}<4$。又由定理9·6及$c=\frac{b^2-d}{4a}\leqslant a$，则得到下

列三个已化型：

{1，0，9}，{2，2，5}，{3，0，3}

2. 把$(x_0, y_0, 3x_0y_0 - z_0)$代(a)的$(x, y, z)$，得

$$x_0^2 + y_0^2 + (3x_0y_0 - z_0)^2 = x_0^2 + y_0^2 + z_0^2 + 9x_0^2y_0^2 - 6x_0y_0z_0 = 3x_0y_0(3x_0y_0 - z_0)$$

所以$(x_0, y_0, 3x_0y_0 - z_0)$亦是(a)的解。

因(1，1，1)是(a)的一个解，按(b)及 x，y，z 的对称性，可以推得，$0 < x \leqslant y \leqslant z$ 的(a)的一切解如下表：

z	1	2	5	13	29	34	89	169	194	233	433	610	985
y	1	1	2	5	5	13	34	29	13	89	29	233	169
x	1	1	1	1	2	1	1	2	5	1	5	1	2

其实际计算方法是，由于

$$x^2 - 3xyz + x^2 + y^2 = 0 \Longrightarrow 2z = 3xy \pm \sqrt{9x^2y^2 - 4(x^2 + y^2)}.$$

若

$$2z = 3xy - \sqrt{9x^2y^2 - 4(x^2 + y^2)}$$

则因$8x^2y^2 - 4x^2 - 4y^2 = 4x^2(y^2 - 1) + 4y^2(x^2 - 1) > 0$，

得到

$$2z < 3xy - xy = 2xy \Longrightarrow z < xy$$

但根据题目的要求，有

$$3xyz = x^2 + y^2 + z^2 \leqslant 3z^2 \Longrightarrow xy \leqslant z$$

矛盾。故只能按

$$2z = 3xy + \sqrt{9x^2y^2 - 4(x^2 + y^2)} > 3xy$$

来计算。

注意：这也是一种递降法，幸有一解 $x = y = z = 1$ 已无法再降。故费马无穷递降法一种可以证明无解，一种可证明有无穷多解。（实际

上，此就是用递降的反向，“递升”到无穷多个解。）

3. 把(c)代入(b)得

$$x_{1,0}^2+\cdots+x_{n-1,0}^2+(nx_{1,0}\cdots x_{n-1,0}-x_{n,0})^2$$

$$=x_{1,0}^2+\cdots+x_{n,0}^2+n^2x_{1,0}^2\cdots x_{n-1,0}^2-2nx_{1,0}\cdots x_{n,0}$$

$$=nx_{1,0}\cdots x_{n-1,0}(nx_{1,0}\cdots x_{n-1,0}-x_{n,0})$$

故结论正确。

4 因为 $x_4=2x_1x_2x_3+\sqrt{4x_1^2x_2^2x_3^2-(x_1^2+x_2^2+x_3^2)}$，且 (1，1，1，1)是

$$x_1^2+x_2^2+x_3^2+x_4^2=4x_1x_2x_3x_4 \tag{c′}$$

的一个解。仿第2题知：(1，1，1，3)，(1，1，3，11)，(1，3，13，131)是(c′)的另三个解。

5. 右边展开整理后，立即得到该恒等式。

6. (1)可用行列式表示于下：

$$\begin{vmatrix} w & 3z & -3y \\ -z & w & 3x \\ y & -x & w \end{vmatrix}=0. \tag{1′}$$

故(1′)的列向量线性相关，即存在不全为0的a，b，c，且(a，b，c)=1，使

$$\begin{cases} wa+3zb-3yc=0 \\ -za+wb+3xc=0 \\ ya-xb+wc=0 \end{cases} \tag{3}$$

(3)是一个四元三个方程的线性方程组。解之就得到w，x，y，z如同(2)的形式，其中ρ是任意有理数。

7. 在第6题(1)中取

$$\begin{cases} w=\frac{1}{2}(\alpha+\beta+\gamma+\delta), & x=\frac{1}{2}(\alpha+\beta-\gamma-\delta) \\ y=\frac{1}{2}(\alpha-\beta+\gamma-\delta), & z=\frac{1}{2}(\alpha-\beta-\gamma+\delta) \end{cases} \tag{5}$$

即得等式(4)。解线性方程组(5)得

$$\begin{cases} \alpha=\frac{1}{2}(w+x+y+z), & \beta=\frac{1}{2}(w+x-y-z) \\ \gamma=\frac{1}{2}(w-x+y-z), & \delta=\frac{1}{2}(w-x-y+z) \end{cases} \quad (6)$$

再把上题的(2)代入(6)就得到(4)的有理数解。

(4)的所有有理数解是可以给出的，其方法是由Enler－Benit给出的

$$\alpha=\sigma[(-\xi-3\eta)(\xi^2+3\eta^2)+1]$$

$$\beta=\sigma[(\xi+3\eta)(\xi^2+3\eta^2)-1]$$

$$\gamma=\sigma[(\xi^2+3\eta^2)^2-(\xi+3\eta)]$$

$$\delta=\sigma[(\xi^2+3\eta^2)^2-(\xi-3\eta)]$$

若$\sigma=1$，ξ，η为整数时，可得(4)的无穷多个整数解，但不是所有的整数解。至于所有的整数解至今尚未给出一般的公式。

8. 由定理9·26系2的证明(iii)中知道，

$$x^2+3y^2=(\alpha_1^2+3\beta_1^2)(\alpha_2^2+3\beta_2^2)=(\alpha_1\alpha_2+3\beta_1\beta_2)^2+$$
$$+3(\alpha_1\beta_2-\alpha_2\beta_1)^2 \quad (a)$$

且$x^2+3y^2=4m$的解数T是

$$\alpha_1^2+3\beta_1^2=2^2 及 \alpha_2^2+3\beta_2^2=m \quad (b)$$

的解数T_1，T_2之积的一半，即$T=\frac{1}{2}T_1T_2$。而$T_2=2E(m)$。

由于题目的要求(b)的第一方程只能是α_1，β_1同为奇数，即$(\alpha_1, \beta_1)=(\pm1, \pm1)$四个解，才能使(a)右边的第一项是奇数。又由于

$$[(\pm1)(\pm\alpha_2)+3(\pm1)(\pm\beta_2)]^2+3[(\pm1)(\pm\beta_2)-(\pm1)(\pm\alpha_2)]$$

$$=[(\pm\alpha_2)+3(\pm\beta_2)]^2+3[(\pm\beta_2)-(\pm\alpha_2)]$$

故实际上，该方程的解数$T=\frac{1}{2}T_2=E(m)$

9. (i) 应用本章第一节的等式(5)（等号改为关于模q同余）经计算得

$d_1 \equiv (ru-st)^2(b^2-4ac) \equiv (ru-st)^2 d \pmod q$

(ii) 由同余式(3)及勒让得符号的性质，得

$$\left(\frac{d}{p}\right)=\left(\frac{d_1}{p}\right)$$

(iii) 因$(p, d)=1 \Longrightarrow p \nmid (a, b, c)$

若 $p \nmid a$，则取 $X \equiv 2ax+by$，$Y=y \pmod p$，则

$ax^2+bxy+cy^2 \equiv 4a^2x^2+4abxy+4acx \equiv (2ax+by)^2-dy^2$

$$\equiv X^2-dY^2 \pmod p$$

若$p \nmid c$，可类似地证之。

若 $p \mid (a, c)$，而 $p \nmid b$，则令$x=X+Y$，$y=XY-Y$，得

$ax^2+bxy+cy^2 \equiv bxy \equiv bX^2-bY^2 \pmod p$

(iv) 令x为过模p的完全剩余系，则ax^2和$1-cy^2$各有$(p+1)/2$个互不同余的值。故必有一组x，y使

$ax^2 \equiv 1-cy^2 \pmod p$

(v) 因为 $p \nmid ac$，$p \mid b$，由(iv)知道存在 r，t 使得 $1 \equiv ar^2+$ $+bt^2 \pmod p$，设s,u是任何一对使 $p \nmid \gamma u-st$的整数,固定 s,u而命

$b_1 \equiv 2ar_s+2ctu$，$c_1 \equiv as^2+cu^2 \pmod p$

则必有 $\{a, o, c\} \sim \{1, b_1, c_1\} \pmod p$。若后者的判别式 $d_1=b_1^2-4c_1$，由(iii)知，

$\{1, b_1, c_1\} \sim \{1, 0, -d_1\} \pmod p$

若 $\left(\frac{d}{p}\right)=1$，由(ii)知 $\left(\frac{d_1}{p}\right)=1$，即$\alpha^2 \equiv d_1 \pmod p$有解。

令$X'=X$，$Y'=\alpha Y$，得

$\{a, b_1, c\} \sim \{1, 0, -d\} \sim \{1, 0, -1\} \pmod p$

取$X'=X''+Y'=X''-Y''$，则

$X'^2-Y'^2 \equiv 4X''Y''Y \equiv X''Y'' \pmod p$

即 $\{1, 0, -1\} \sim \{0, 1, 0\} \pmod p$。

类似地，可证明本题的其余部分。

(vi) 由定义此题即 $ru-st=1$的情况，故结论成立。